www.tecChannel.de April/Mai/Juni 02/2003

NEU!

# tecCHANNEL COMPACT

KOMPENDIUM FÜR IT-PROFIS

€ 9,90
Österreich € 10,90
Benelux € 11,40
Schweiz SFR 19,80

# IT-Security

## Viren · SPAM · Clients · Datensicherheit · Netze · Server

Unentbehrliches Know-How für den IT-Profi

Grundlagen, Konzepte und Workshops für mehr Desktop- und Netzwerk-Sicherheit

### XP-Dienste optimieren

Services richtig konfigurieren und kritische Funktionen abschalten

### SPAM-Abwehr

Schützen Sie Ihr Netzwerk vor unerwünschten Massenmails

### Ausfallsichere Systeme

Desktops, Web- und Fileserver auf mehr Zuverlässigkeit trimmen

### PKI im Unternehmen

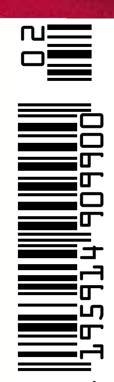
Authentifizierung & Verschlüsselung zentral planen und managen

### WLANs absichern

So umgehen Sie die Schwächen des WLAN-Standards

### Die Portreferenz

Die wichtigsten TCP/IP-Ports und Funktionen zur Firewall-Konfiguration



# Editorial

## Sicherheit durch Technik und Management

„Nie war eine sichere IT-Plattform so wichtig wie heute, da wir zunehmend über das Internet kommunizieren und unsere Geschäfte abwickeln. Die bessere Kommunikation bringt zwar erhebliche Vorteile mit sich, aber auch Sicherheitsrisiken in einem Ausmaß, das nur wenige vorausgesehen haben.“ Mit diesen Worten wandte sich Bill Gates am 23. Januar 2003 in einer E-Mail an die Microsoft-Kunden, um eine neue Runde der Trustworthy-Computing-Initiative einzuläuten.

Wie zum Beweis brach keine 48 Stunden später das Internet für einen halben Tag komplett zusammen. Fünf der dreizehn Root-DNS-Server fielen aus, auf den Backbones der großen Provider ging ständig rund ein Drittel der Pakete verloren. Auslöser des Chaos war der nur 376 Byte große Slammer-Wurm, der binnen drei Minuten nach seiner Freisetzung Zehntausende von MS-SQL-Servern infizierte und einen massiven Denial-of-Service-Zwischenfall verursachte.

War Slammer ein Einzelfall? Nein – das belegen einschlägige Studien der Security-Industrie. Angriffe mit hybriden, sich blitzartig ausbreitenden Schädlingen werden 2003 die Regel sein. Als Einfallstore ins Unternehmen dienen dabei neben E-Mails zunehmend Sicherheitslücken in Betriebssystemen und Applikationen. Um die Firmen-IT zu schützen, genügen künftig selektive Einzelmaßnahmen an der Peripherie, wie Firewalls oder SMTP-AV-Scanner, nicht mehr. Es gilt, Rechner und Infrastruktur vorbeugend gegen Attacken zu härten und diese technischen Präparationen mit umfassenden organisatorischen Maßnahmen zu flankieren.

Der vorliegende vierte Band der tecCHANNEL-Compact-Reihe gibt Ihnen dazu die wichtigsten Informationen und Techniken an die Hand. Die Bandbreite reicht von Maßnahmen zum Härten der Clients über die Grundlagen des Firewall-Einsatzes bis hin zur Absicherung des Unternehmens mit einer eigenen PKI. Doch Sicherheit ist nicht allein ein technischer Zustand, sondern vor allen Dingen ein laufender Prozess. Deswegen empfehlen wir Ihnen ganz besonders die Lektüre der Kapitel über Security in mittelständischen Betrieben und über Notfallplanung.

Wir hoffen, dass Ihnen unser Security-Compact dabei hilft, dieses Jahr ohne ärgerliche und kostspielige Sicherheitszwischenfälle zu überstehen, und wünschen Ihnen eine anregende Lektüre.

Jörg Luther

Redakteur Software & Netzwerke

Wir freuen uns über Kritik und Anregungen zu dieser Compact-Ausgabe. Unter www.tecChannel.de/compact können Sie uns per Fragebogen Feedback geben.

# Impressum

Chefredakteur: Michael Eckert (mec), (verantwortlich, Anschrift der Redaktion)
Chef vom Dienst: Kerstin Lohr
Grafik: stroemung, Köln, Michael Rupp, Oliver Eismann, h2design, München, Yvonne Reittinger

**Redaktion tecCHANNEL:**

Leopoldstraße 252b, 80807 München, Tel. 0 89/3 60 86-897, Fax: -878

Homepage: www.tecChannel.de, E-Mail: redtecchannel@idginteractive.de

Autoren dieser Ausgabe :
Mike Hartmann, Albert Lauchner, Jörg Luther, Klaus Manhardt, Konstantin Pfliegl, Thomas Rieske, Detlef Schumann, Axel Sikora

Textredaktion: Kerstin Lohr



**Anzeigen:**
Anzeigenleitung: Dominique Remus, Tel.: 0 89/3 60 86-871
Leitung Anzeigendisposition: Rudolf Schuster, Tel. 0 89/3 60 86-135, Fax -328
Anzeigentechnik: Martin Mantel, Andreas Mallin
Digitale Anzeigenannahme: Thomas Wilms, leitend, Tel. 0 89/3 60 86-604, Fax -328

**Vertrieb:**
Vertriebsleitung: Josef Kreitmair
Vertriebsmarketing: Peter Priewasser (leitend), Stefanie Kusseler
Vertrieb Handelsauflage: MZV Moderner Zeitschriften Vertrieb, Breslauer Straße 5, 85386 Eching, Tel.: 0 89/3 19 06-0, Fax: -113, E-Mail: mzv@mzv.de, Website: www.mzv.de
Produktionsleitung: Heinz Zimmermann

**Druck:** Schoder Druck, Gutenbergstraße 12, 86368 Gersthofen


**Verlag:**
IDG Interactive GmbH, Leopoldstraße 252b, 80807 München, Tel.: 0 89/3 60 86-0, Fax: -501

**Leserservice:**
A.B.O Verlagsservice GmbH, Ickstattstraße 7, 80469 München, Tel: 0 89/20 95 91 32, Fax: 0 89/20 02 81 11

**Geschäftsführer:** York von Heimburg
Verlagsleitung: Frank Klinkenberg
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: Alleiniger Gesellschafter der IDG Interactive GmbH ist die IDG Communications Verlag AG, München, eine 100-prozentige Tochter der IDG Inc., Boston, Mass., USA.

**Vorstand:** Keith Arnot, York von Heimburg, Ralph Peter Rauchfuss

**Aufsichtsratsvorsitzender:** Patrick McGovern

# Inhalt

# 1 Grundlagen

Bei der Absicherung eines Netzwerks kommen eine Vielzahl von Verfahren und Standards zum Einsatz. Im ersten Abschnitts unseres Compacts finden Sie Grundlagen und Informationen zu den wichtigsten Sicherheitsverfahren, wie Verschlüsselungstechnologien und deren Einsatzgebieten oder dem prinzipiellen Aufbau und der Funktionsweise von Public-Key-Infrastrukturen und Firewall-Systemen. Eine Übersicht der gängigsten Angriffsverfahren hilft bei der Gefahrenanalyse.

## 1.1 Kryptographie im Überblick

Mit der steigenden Verbreitung computer- und netzwerkgestützter Anwendungen gewinnt die Frage der Computer- und der Netzwerksicherheit immer größere Bedeutung. Dies ist vor allem auf fünf Aspekte zurückzuführen:

- Die Nutzung von öffentlichen Netzwerken durch Laien führt dazu, dass zahlreiche unzureichend konfigurierte und damit relativ ungeschützte Systeme im Netz eine breite Angriffsfläche bieten.
- Automatisierte, im Internet verbreitete Werkzeuge – oft sogar mit grafischen Oberflächen – machen die Vorbereitung und Ausführung eines Angriffs sehr einfach. Das Hacken im Netz entwickelt sich zunehmend von einer Spezialistendisziplin zum Kinderspiel.
- Auf Grund immer kürzerer Entwicklungszyklen (Stichwort: Time to Market) weisen alle Software-Lösungen mehr oder weniger gravierende Sicherheitslücken auf. Ein Nachführen von Bugfixes und Patches fällt wegen der Masse speziell Netzwerkadministratoren zunehmend schwerer.
- Definition, Implementierung und Einsatz von Sicherheitskonzepten gestalten sich in der Regel komplex. Statt definierte, maßgeschneiderte Lösungen aufzusetzen, begnügen sich viele Anwender mit dem Einsatz proprietärer und isolierter Produkte. Ein trügerisches Gefühl von Sicherheit ist die Folge.
- Der mobile Einsatz von Rechnern nimmt stetig zu. Besonders drahtlose Übertragungstechniken, aber auch der wachsende Einsatz von Remote Access (Dial-In/VPN) schaffen neue Herausforderungen an Sicherheitsarchitekturen.

### 1.1.1 Safety und Security

Im Zusammenhang mit Rechnern und Netzen lässt sich Sicherheit als Nichtvorhandensein von Gefahren oder wirksamer Schutz vor Risiken beschreiben. Damit handelt es sich um eine nur subjektiv wahrnehmbare Größe, die man weder direkt sehen noch messen kann.

Die englische Sprache bietet die im Deutschen leider fehlende Unterscheidung zwischen Safety und Security, die zwei verschiedene Aspekte von Sicherheit näher eingrenzt. Safety bezieht sich auf die Zuverlässigkeit eines Systems, speziell in Bezug auf dessen Ablauf- und Ausfallsicherheit. Security bezeichnet dagegen den Schutz eines Systems vor beabsichtigten Angriffen. Die beiden Begriffe sind nicht völlig unabhängig voneinander: Safety schließt auch Security mit ein.

Unsere Artikelserie zum Thema Sicherheit konzentriert sich auf den Aspekt der Security und beschäftigt sich dabei mit folgenden Unterthemen:

- Vertraulichkeit (Confidentiality, Privacy): Sicherheit gegen Angriffe durch unerlaubtes Abhören
- Integrität (Integrity): Schutz gegen die (meist partielle) Veränderung von Informationen. In Netzwerken kann sich die Integrität sowohl auf die Inhalte von Datenpaketen als auch auf deren Steuerinformationen und hierbei insbesondere auf die Adressierung beziehen.
- Authentifizierung (Authentication, auch Non-Repudiation): Überprüfung, ob ein Sender wirklich derjenige ist, der er zu sein vorgibt.
- Verfügbarkeit (Availability) und Zugang (Access): Informationen sind nur dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

Der hier vorliegende erste Teil der Serie beschäftigt sich mit der Sicherstellung der Vertraulichkeit: Wir werfen einen näheren Blick auf die Grundlagen und die einzelnen Verfahren der Kryptographie.

### 1.1.2 Kryptographie

Das Wort Kryptographie ist aus den griechischen Wörtern krypto (Griech.: versteckt, geheim) und graph (Griech.: Schrift, Wort) entlehnt. Damit bedeutet Kryptographie im Ursprung so viel wie Geheimschrift.

Kryptographie behandelt zum einen die Verschlüsselung (Encryption), also die Transformation einer verständlichen Informationsdarstellung (Klartext, Plain Text, Clear Text) in eine nicht verständliche Darstellung (verschlüsselter Text, Geheimtext, Cipher Text). Diese muss in einer Weise erfolgen, dass die angewandte Transformation im Rahmen einer Entschlüsselung (Decryption) von Befugten wieder eindeutig rückgängig gemacht werden kann.

Vor Dritten wird also nicht die Existenz der eigentlichen Information versteckt, sondern man versteckt lediglich deren Bedeutung. Diesen Aspekt der Vertraulichkeit bezeichnet man auch als Konzelation. Mit dem Verbergen von Informationen beschäftigt sich eine spezielle Variante der Kryptographie, die so genannte Steganographie (steganos, Griech: bedeckt).

Im erweiterten Sinne zählen zur Kryptographie auch Aufgaben der Integritätsprüfung und Authentifizierung. Oft basieren entsprechende Funktionen auf eingeschränkten kryptographischen Verfahren, bei denen die Verschlüsselung nicht

unbedingt rückgängig gemacht werden muss. Hier muss lediglich sichergestellt werden, dass zwei unterschiedliche Eingaben nur mit einer sehr geringen Wahrscheinlichkeit das gleiche Ergebnis liefern.

### 1.1.3 Transposition vs. Substitution

In der Kryptographie unterscheidet man zwei grundsätzliche Schlüsselverfahren. Die Transposition ändert die Anordnung der Zeichen in der Folge, lässt das Auftreten der Zeichen jedoch unverändert. Dies kann man beispielsweise dadurch erreichen, dass man jeweils zwei aufeinander folgende Buchstaben austauscht: Aus *Kryptographie* wird dann *Rkpyotrgpaihe*.

Als Scrambling („Verwürfeln") wird Transposition auch bei vielen drahtlosen Übertragungstechniken eingesetzt. Dort entschärft sie den Einfluss von Büschelfehlern (Burst Errors), die mehrere aufeinander folgende Zeichen in der Übertragung stören. Nach dem „Descrambeln" folgen die gestörten Bereiche nicht mehr unmittelbar aufeinander. Sie verteilen sich über einen größeren Bereich, so dass Fehlererkennungs- und Korrekturmechanismen besser greifen.

Das zweite grundsätzliche Kryptverfahren, die Substitution, ersetzt Zeichen des Klartextes im Geheimtext durch andere Zeichen. Ein einfaches Beispiel dafür ist die vom gleichnamigen römischen Kaiser gern verwendete Cäsar-Addition. Sie ersetzt jeden Buchstaben des Klartextes durch den, der im Alphabet drei Plätze weiter hinten steht. So wird aus *Kryptographie* der Chiffretext *Nucswrjudsklh*.

### 1.1.4 Symmetrische Substitution

Die symmetrische Substitution verdankt ihren Namen der Tatsache, dass Sender und Empfänger im Besitz des gleichen Schlüssels sein müssen, um vertraulich miteinander zu kommunizieren. Außer den beiden Kommunikationspartnern darf niemand den Schlüssel kennen (Secret-Key-Verfahren).

Symmetrische Verfahren erreichen auch bei der Implementierung als Software akzeptable Verschlüsselungsraten. Sie eignen sich deshalb besonders gut zur Verschlüsselung großer Datenmengen. Der große Nachteil: Um die Nachrichten verwerten zu können, muss der Empfänger in den Besitz des verwendeten Schlüssels gelangen. Die Übertragung des Schlüssels stellt einen Schwachpunkt dar, an dem ein Angreifer ansetzen kann.

Zudem brauchen je zwei miteinander kommunizierende Partner einen exklusiven, geheimen Schlüssel. Die Anzahl der benötigten Schlüssel m hängt quadratisch von der Anzahl n der kommunizierenden Partner ab (m = 0,5 * n * (n-1)).

## 1.1.5 Symmetrische Substitutionsverfahren

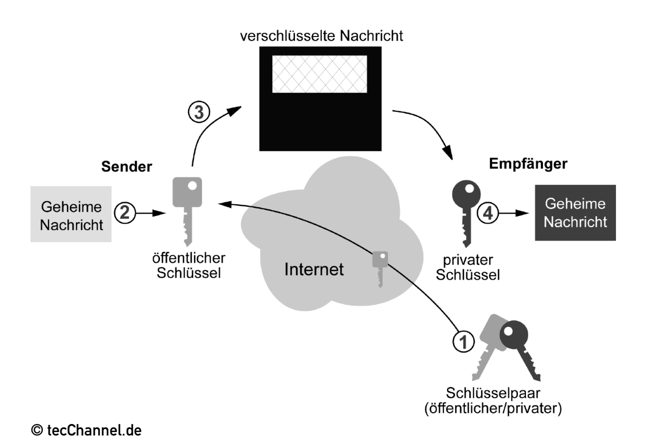
Symmetrische Verfahren lassen sich nach Zeichen-, Block- und Stromchiffren klassifizieren. Die zeichenorientierte Substitution ermittelt jedes Zeichen des Geheimtexts aus dem entsprechenden Zeichen des Klartextes unter Zuhilfenahme des Schlüssels. Das einfachste und bekannteste Beispiel dafür ist die bereits erwähnte Cäsar-Chiffrierung.

Stromchiffrierung verschlüsselt den Klartext Byte-weise über eine XOR-Operation. Dazu erzeugt sie in Abhängigkeit vom gewählten Schlüssel eine sich zyklisch verändernde Byte-Folge, die mit dem Klartext verknüpft wird. Durch ein erneutes XOR kann der Empfänger den Klartext rekonstruieren. Das macht Stromverschlüsselung sehr schnell, zudem lässt sie sich ideal in Software implementieren. Das bekannteste Beispiel einer Stromchiffrierung ist der RC4-Algorithmus.

Die blockorientierte Substitution fasst Bitgruppen des Klartexts in Blöcken zusammen und transponiert diese mittels in der Regel mehrstufiger Verfahren anhand des Schlüssels über gleichbleibende Operationen in den Geheimtext. Die bekannteste Blockchiffrierung ist DES.

## 1.1.6 Asymmetrische Substitution

Eine elegante Alternative zu den symmetrischen Kryptverfahren bietet die so genannte asymmetrische Verschlüsselung. Sie verwendet zwei komplementäre Schlüssel, die so ausgewählt werden, dass mit dem einem Key chiffrierte Nachrichten nur mit dem zweiten Key wieder dechiffriert werden können. Einen der beiden Schlüssel kann man also gefahrlos öffentlich bekannt geben, weswegen man diese Vorgehensweise auch als Public-Key-Verfahren bezeichnet.




**Public-Key-Verfahren:** Mit dem öffentlichen Schlüssel des Empfängers lassen sich Nachrichten so verschlüsseln, dass sie auch nur mit dessen privatem Schlüssel wieder zu entziffern sind.

Den privaten zweiten Schlüssel nennt man Private Key, den frei zugänglichen logischerweise Public Key. Eine mit dem öffentlichen Schlüssel chiffrierte Nachricht kann nur mit dem privaten Schlüssel dechiffriert werden. Anders herum gilt auch, dass sich eine mit dem Private Key chiffrierte Nachricht nur mit dem öffentlichen Schlüssel dechiffrieren lässt.

Public-Key-Chiffrierungen basieren auf einem mathematischen Bezug zwischen den verwendeten privaten und öffentlichen Schlüsseln. Dieser muss so komplex sein, dass Außenstehende nicht aus der Kenntnis des Public Key auf den passenden Private Key schließen können.

### 1.1.7 Vorteile von Public-Key-Verfahren

Die Verwendung von Public Keys bringt vor allem den Vorteil, dass jeder Kommunikationspartner nur einen Schlüssel (seinen Private Key) benötigt. Als zweiten Schlüssel kann er den Public Key der Gegenstelle einsetzen, der ja öffentlich bekannt ist. Das entschärft das Skalierungsproblem der symmetrischen Verschlüsselungsverfahren ganz wesentlich.

Als Nachteil handelt man sich andererseits bei den Public-Key-Verschlüsselungen eine hohe Komplexität der durchzuführenden Operationen ein. Die meisten asymmetrischen Substitutionsverfahren beruhen auf mathematischen Funktionen wie der Multiplikation oder der Exponentialfunktion. Die Multiplikation zweier Zahlen stellt eine einfache Operation dar, während der umgekehrte Vorgang, also die Faktorzerlegung eines Produkts, einen enormen Rechenaufwand bedeuten kann.

Dies gilt insbesondere dann, wenn das Produkt wie beim RSA-Verfahren in seine Primfaktoren zerlegt werden muss. Gleiches gilt für die Exponentialfunktion, deren Berechnung vergleichsweise einfach erfolgt. Die Berechnung der inversen Exponentialfunktion wiederum weist eine sehr hohe Komplexität auf.

### 1.1.8 Absicherung der asymmetrischen Substitution

Eine wesentliche Schwäche des Public-Key-Verfahrens besteht in der a priori nicht eindeutigen Zuordnung des öffentlichen Schlüssels zu seinem Besitzer. Auf diese Weise könnte sich ein „Man-in-the-Middle“ in die Kommunikation zwischen Alice und Bob so einschalten, dass er Nachrichten von beiden entschlüsseln kann, ohne dass diese es bemerken.

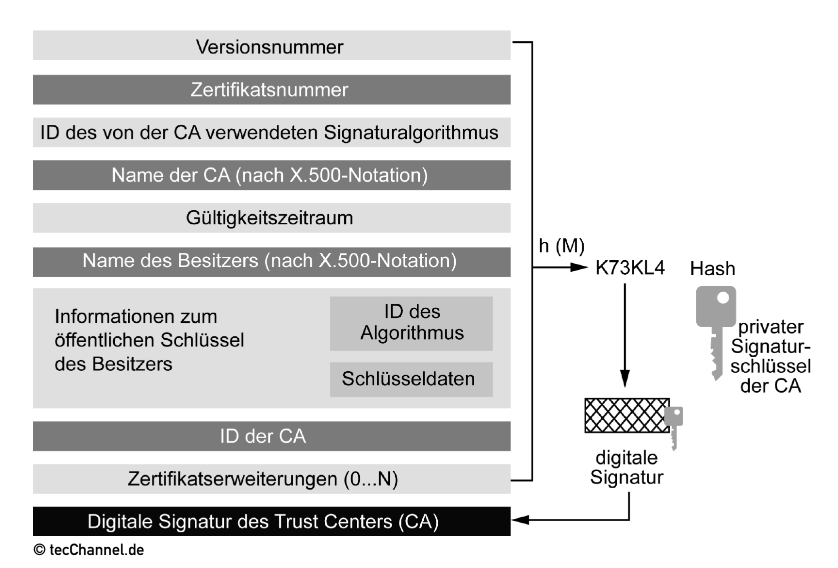
Daher ist es von zentraler Bedeutung, dass die Information über den öffentlichen Schlüssel und den zugehörigen Besitzer von einer vertrauenswürdigen Quelle stammt. Hierzu existieren im Rahmen einer so genannten Public Key Infrastructure (PKI) verschiedene Möglichkeiten:

So kann man zum einen den öffentlichen Schlüssel über ein als sicher betrachtetes Medium übertragen. Darunter fällt speziell die persönliche Übergabe, aber auch

die Übermittlung per Telefon, Brief oder Fax haben sich trotz aller Einschränkungen etabliert. Zum anderen besteht die Möglichkeit, sich die Identität des Schlüsselinhabers von einer Zertifizierungsstelle bestätigen zu lassen.

## 1.1.9 Trust Center

Zur Überprüfung der Schlüsselinhaber dient meist eine Zertifizierungsinstanz, (Englisch: Certification Authority (CA)), manchmal auch als Trust Center bezeichnet. Über die CA können sowohl Alice als auch Bob überprüfen, ob ein zur Beglaubigung eingereichter öffentlicher Schlüssel und eine Person mit einem eindeutigen Namen wirklich zusammengehören.




**Aufbau eines Zertifikats:** Die digitale Signatur der CA stellt sicher, dass der Schlüssel auch zum angegebenen Inhaber gehört.

Dazu verwalten Alice und Bob eine Liste von Zertifizierungsinstanzen, bei denen der Zusammenhang zwischen einem empfangenen öffentlichen Schlüssel und dessen Absender überprüft werden kann. Die Zertifizierungsinstanz stellt auf Anfrage ein Zertifikat nach dem ITU-Standard X.509 aus. Die obige Abbildung zeigt das in PKCS#6 definierte X.509-Format in der Version 3, das viele kryptographische Protokolle im Internet einsetzen.

Die Überprüfung des Schlüsselinhabers erfolgt meist transparent für den Anwender. Nur wenn beim Trust Center kein öffentlicher Schlüssel hinterlegt ist, müssen Alice oder Bob manuell entscheiden, ob sie die Kommunikation weiterführen.

Als weniger aufwendige Alternative zur Verwendung einer CA besteht die Möglichkeit, sich die Authentizität eines öffentlichen Schlüssels durch einen bereits bekannten, zertifizierten Kommunikationspartner bestätigen zu lassen. Diesen Weg nutzt beispielsweise PGP zum Aufbau eines so genannten Web of Trust.

## 1.1.10 Hash-Funktionen

Die Bezeichnung „Hash-Funktionen" leitet sich vom englischen „to hash up" (zerhacken, zerkleinern, durcheinander bringen) ab. Synonym spricht man auch vom „Message Digest", Engl.: digest, Auslese, Auswahl) oder kurz MD. Eine Hash-Funktion generiert aus einer Zeichenfolge beliebiger Länge eine zweite Zeichenfolge fixer Länge. Diese zweite Zeichenfolge bezeichnet man als Message Authentication Code (MAC).

Eine Hash-Funktion muss dabei folgende Anforderungen erfüllen:

- Sie muss eindeutig sein. Eine identische Eingangszeichenfolge muss zur selben Zeichenfolge am Ausgang führen.
- Sie muss einfach zu berechnen sein.
- Ihre inverse Funktion muss schwierig zu berechnen sein. Ein Rückschluss aus der Ausgangszeichenfolge auf die Eingabe soll also möglichst aufwendig sein.
- Sie muss kollisionsresistent sein. Zwei unterschiedliche Eingangszeichenfolgen dürfen nach Möglichkeit nicht die gleiche Ausgabe hervorrufen.

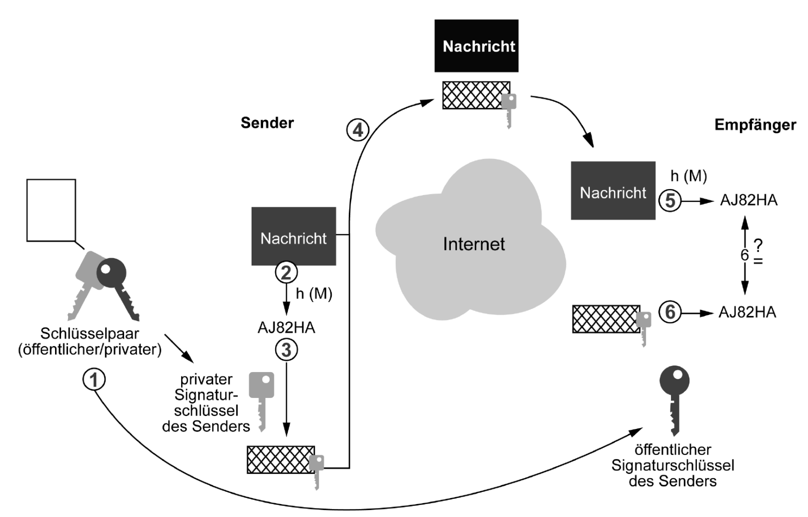
Da Hashes nicht reversibel sind, lassen sie sich nicht zur Verschlüsselung einsetzen. Dagegen leisten sie bei der Authentifizierung nützliche Dienste. So legt man Passwörter gern als MAC ab, damit sie auch der Administrator nicht als Klartext lesen kann. Das Login überprüft dann lediglich, ob der MAC des eingegebenen Passworts mit dem abgelegten Hash-Wert übereinstimmt. Auch für digitale Unterschriften (Digital Signatures) lässt sich ein MAC bestens einsetzen.

## 1.1.11 Substitution vs. Signatur

Die Algorithmen asymmetrischer Verschlüsselung unterscheiden sich grundsätzlich. Dies hängt davon ab, ob eine Nachricht verschlüsselt oder signiert wird.

Bei der Substitution verschlüsselt der Sender die Nachricht mit dem öffentlichen Schlüssel des Empfängers, so dass dieser die Nachricht mit Hilfe seines privaten Schlüssels wieder in Klartext übersetzen kann.

Bei der Authentifizierung dagegen erzeugt der Absender mit Hilfe seines privaten Schlüssels eine Signatur, die der Empfänger unter Verwendung des öffentlichen Schlüssels des Senders verifizieren kann.




**Signieren mit dem Public Key:** Der Absender unterzeichnet seine Nachricht mit dem Private Key. Mit dem Public Key kann der Empfänger die Authentizität der Unterschrift prüfen.

## 1.1.12 Hybride Verschlüsselungsverfahren

Sowohl die symmetrischen als auch die asymmetrischen Kryptverfahren bringen ganz spezifische Vor- und Nachteile mit sich. Das legt den Gedanken nahe, in Anwendungslösungen zur Verschlüsselung beide Varianten zu verbinden.

Die resultierenden hybriden Verschlüsselungen verbinden die Vorteile der symmetrischen und der asymmetrischen Methode: Also die hohe Effizienz auf der einen Seite und die Flexibilität und gesteigerte Sicherheit auf der anderen Seite.

Hierbei kommen in der Regel die symmetrischen Algorithmen zur Verschlüsselung größerer Datenmengen zum Einsatz. Der Austausch der hierzu notwendigen Schlüssel erfolgt dann über ein asymmetrisches Verfahren.

## 1.1.13 Ende-zu-Ende vs. abschnittsweise Sicherheit

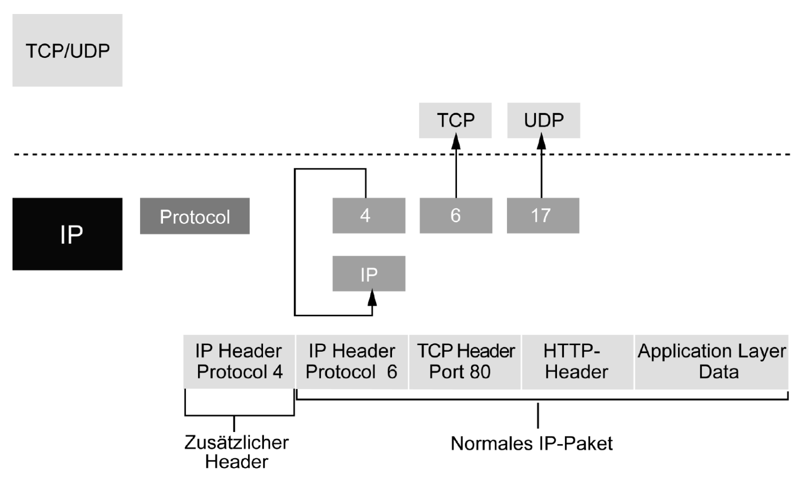
Ende-zu-Ende-Sicherheitsarchitekturen gehen davon aus, dass zwei Endgeräte einen sicheren Kanal aushandeln, aufbauen und aufrecht erhalten. Alternativ kann man aber nur kritische Übertragungsstrecken durch Verschlüsselung absichern. Ein Beispiel dafür wäre die Kommunikation zwischen zwei Mailservern, bei denen die lokale Datenübertragung mit den Mail-Clients unverschlüsselt erfolgt.

Die Vor- und Nachteile der beiden Architekturen sind offensichtlich:

- Ende-zu-Ende-Sicherheit bietet in der Regel eine geringere Angriffsfläche, stellt aber meist hohe Anforderungen an die Rechenleistung und die Konfiguration der Endgeräte.
- Abschnittsweise Sicherheit bietet mehr Gelegenheit für Attacken, beschränkt die Notwendigkeit hoher Sicherheitsanforderungen aber auf die Gateways.

## 1.1.14 Tunneling

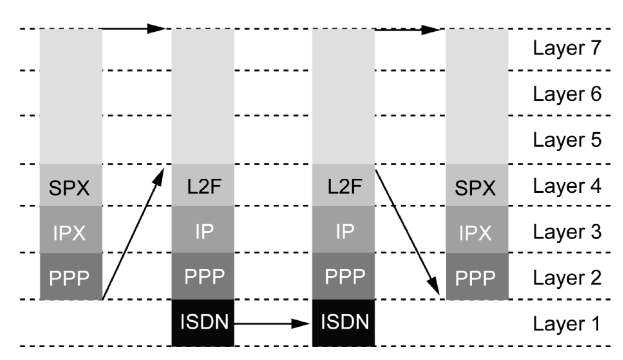
Abschnittsweise Sicherheit wird heute meist über Tunneling realisiert. Darunter versteht man das mehrfache Einpacken eines Pakets auf einer Transportebene.




© tecChannel.de

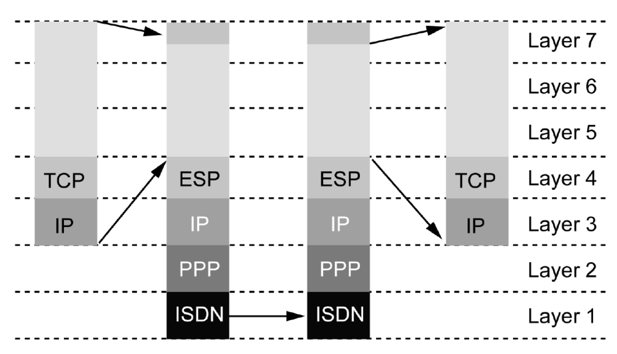
**IP/IP-Tunneling:** Für den Transport über klassische IP-basierte Netze kann man IPv6 über IPv4 tunneln.

Dazu ein kleines Beispiel: Ein TCP-Paket kann man in ein IP-Paket verpacken, indem man einen IP-Header mit den notwendigen Steuerinformationen (Quelladresse, Zieladresse, TTL et cetera) hinzufügt. Dabei setzt man das Type-Feld auf den Wert 6, damit das empfangende IP-Modul nach dem Entfernen des IP-Headers das TCP-Empfangsmodul aufruft.




**Layer-2-Tunneling:** Pakete der OSI-Schicht 2, meist PPP-Frames, werden in IP-Pakete verpackt. So tunnelt man üblicherweise alle Nicht-IP-Protokolle.

Beim Tunneln verpackt man das IP-Paket in ein weiteres, indem man einen zweiten IP-Header voranstellt. Damit beim Auspacken eine eindeutige Zuordnung erfolgen kann, setzt man das Type-Feld auf den Wert 4. Das empfangende IP-Modul ruft sich dann nach dem Entfernen des äußeren IP-Headers noch einmal auf.




**Layer-3-Tunneling:** Pakete der Vermittlungsschicht werden in IP-Frames verpackt. Bekanntestes Verfahren dieser Art ist IPsec.

So lässt sich das IP-Paket beispielsweise für normale Router anonymisieren, speziell auch mit anderen Ziel- und Quelladressen versehen.

## 1.1.15 Angriffsverfahren

Sammelt ein Angreifer verschlüsselte Pakete, so kann er über diverse Techniken versuchen, Rückschlüsse auf den Originaltext zu ziehen. Meist steht dazu nur die verschlüsselte Nachricht zur Verfügung. Dies nennt man Cipher-Text-Angriff.

Dazu bieten sich verschiedene Möglichkeiten. Zum einen kann der Angreifer durch unmittelbares Ausprobieren aller Substitutionsmöglichkeiten versuchen, den Klartext zu rekonstruieren.

Die Komplexität des Ausprobierens ist hierbei je nach verwendetem Kryptverfahren mehr oder weniger hoch. Um einen Einblick in die typische Komplexitätsbetrachtung kryptographischer Analyse zu geben, nehmen wir uns einmal die bereits zitierte Cäsar-Chiffre vor.

## 1.1.16 Exhaustive Testing

Wenn wir im Rahmen einer monoalphabetischen Substitution („Cäsar“) jeden Buchstaben eines Alphabets mit 27 Buchstaben (26 plus ein Satzzeichen) einem beliebigen anderen zuordnen, erhalten wir:

- 27 Möglichkeiten für den ersten Buchstaben
- 26 Möglichkeiten für den zweiten Buchstaben
- 25 Möglichkeiten für den dritten Buchstaben
- et cetera...

Das entspricht 27 * 26 * .... * 2 * 1 = 27! oder rund $1{,}09 * 10^{28}$ verschiedenen Zuordnungsmöglichkeiten. Nehmen wir einmal an, das Ausprobieren einer jeden Möglichkeit benötigte 1000 Maschinenzyklen auf einem Pentium-IV-Prozessor, der mit 2,5 GHz getaktet ist und bei jedem Oszillatortakt vier Befehle ausführen kann. Dann dauerte das Durchprobieren aller Möglichkeiten („Exhaustive Testing“) rund 34,5 Billionen Jahre. Zum Vergleich: Der Urknall fand vor 13 bis 14 Milliarden Jahren statt, die Erde ist rund 4,5 Milliarden Jahre alt.

## 1.1.17 Statistische Analyse

Allerdings lassen sich Verschlüsselungen nicht nur durch erschöpfendes Testen knacken. Ein schlauer Angreifer rückt Kryptverfahren durch gezieltes Ausnutzen der Schwachpunkte zu Leibe. So kann man beispielsweise den verschlüsselten Datenverkehr statistisch analysieren.

Im Fall unserer monoalphabetischen Verschlüsselung bedeutet das: Da hier jeder Buchstabe eines Alphabets einem bestimmten anderen zugeordnet wird, bleibt die Häufigkeit des Auftretens der einzelnen Buchstaben erhalten. Somit lassen sich durch eine einfache Häufigkeitsanalyse Rückschlüsse über den ursprünglichen Text ziehen, sofern man dessen Sprache kennt oder erraten kann.

In deutschen Texten tritt etwa der Buchstabe „e“ mit einer mittleren Wahrscheinlichkeit von 17,4 Prozent auf und übertrifft damit alle anderen Buchstaben weit. Findet man also in einem verschlüsselten Text einen Buchstaben, dessen Häufigkeit die der anderen deutlich übersteigt, handelt es sich sehr wahrscheinlich im Klartextalphabet um das „e“. Auch Buchstabenpaare (Bigramme) treten mit unterschiedlichen Häufigkeiten auf: „en“ ist beispielsweise mit 3,9 Prozent das häufigste Bigramm. Mit solchen Kenntnissen ausgestattet, kann ein Angreifer durch statistische Analyse monoalphabetische Codes sehr schnell entschlüsseln.

## 1.1.18 Known oder Chosen Plaintext

Das Knacken von Schlüsseln und Kryptverfahren fällt Angreifern wesentlich leichter, wenn sie Teile des Klartexts bereits vorab kennen. So konnten die Alliierten im Zweiten Weltkrieg die deutschen Enigma-Codes oft auf Grund stereotyper Meldungen brechen: Jeder Spruch begann mit der Buchstabengruppe ANX („an:“) und endete mit HEILHITLER. Bei sehr kurzen Nachrichten durfte man getrost den Inhalt KEINEBESONDERENVORKOMMNISSE als sicher annehmen und konnte daraus den Tages-Code ermitteln.




© tecChannel.de

**Teilweise vorhersagbar:** Speziell die Header-Daten von IP-Paketen lassen sich unschwer erraten oder ermitteln und ermöglichen so Known-Plaintext-Attacken.

Diese Methode funktioniert auch für Datenpakete, bei denen speziell im Header Teile der Information vorhersagbar sind. In den IP-Kopfdaten findet sich an bekannten Stellen als Versionsangabe in der Regel „4“ (IPv4), als Type of Service meist „0“, als Protokollangabe oft „6“ (TCP). Die auch im Header angegebene Paketlänge lässt sich schlicht nachzählen. Besteht zusätzlich die Möglichkeit, den Verkehr nach verschiedenen Routern abzuhören, kennt man auch den Inhalt des TTL-Felds (Anzahl der Hops).

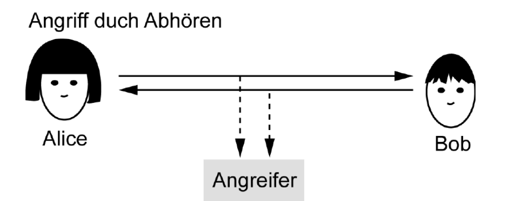
In anderen Fällen besteht für den Angreifer sogar die Möglichkeit, selbst gewählten Text nach den gleichen Regeln wie ein berechtigter Nutzer verschlüsseln zu lassen. Kann der Angreifer anschließend den verschlüsselten Text abhören, besteht natürlich die Möglichkeit, Rückschlüsse über den Verschlüsselungsalgorithmus zu ziehen. Auch dafür ein Beispiel aus dem letzten Krieg: In einem bekann-

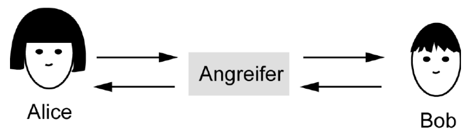
ten Fall bombardierte die britische Luftwaffe eine Markierungsboje, um die vorhersagbare Enigma-chiffrierte Meldung ERLOSCHENISTLEUCHTTONNE zu provozieren. Tages-Code geknackt...

## 1.1.19 Angriffsarten

Ein Angreifer kann verschiedenste Möglichkeiten nutzen, um an die Information einer verschlüsselten Nachricht zu kommen, die von einem Sender A (gern als „Alice“ apostrophiert) an einen Empfänger B („Bob“) geschickt wird.

Die gängigste Methode ist die des Abhörens. Nach dem englischen Verb to eavesdrop (heimlich lauschen) nennt man Lauscher „Eve“. In Netzen, die über Hubs verbunden sind, hört der Angreifer am leichtesten mit: Jedes Datenpaket wird ja an jedem Port ausgegeben. Aber auch in Netzen, die per Switch oder Router gekoppelt sind, können – etwa über Manipulation der Adresstabellen – Datenpakete abgefangen oder umgeleitet werden.




© tecChannel.de

**Die gängigsten Attacken:** Der Angreifer hört die übermittelten Nachrichten passiv mit oder schaltet sich aktiv zwischen Absender und Empfänger.

Über die gezielte Manipulation des Datenverkehrs erfolgt auch der Man-in-the-Middle-Attack. Der Angreifer – hier nennt man ihn „Mallory“ – schaltet sich zwischen Alice und Bob. So kann er Alices Pakete abfangen und mitlesen, bei Bedarf modifizieren, und dann an Bob weiter senden. Verhält Mallory sich dabei konsistent, meinen Alice und Bob, dass sie unmittelbar miteinander kommunizieren. Mallory kann nun  die Wahl der Kryptverfahren oder die Auswahl der Keys so beeinflussen, dass er die Nachrichten von Alice und Bob mitlesen kann.

Replay-Attacken basieren darauf, kritische Teile einer Kommunikation aufzuzeichnen und sie später wieder abzuspielen. Der Angreifer kann etwa eine Login-Prozedur simulieren und so versuchen, ein Passwort herauszufinden.

Weisen die vorangegangenen Verfahren noch eine gewisse Eleganz auf, so operiert der Brute-Force-Angriff mit nackter Gewalt. Der Angreifer bombardiert den Zielrechner beispielsweise mit einer so großen Zahl von Anfragen, dass keine Ressourcen mehr für die Erfüllung der eigentlichen Aufgabe zur Verfügung stehen.

### 1.1.20 Ausblick

Im vorliegenden ersten Teil unserer Security-Grundlagen haben wir einige Basisdefinitionen abgeklärt und uns näher mit den Schlüsselbegriffen der Kryptologie und Kryptanalyse vertraut gemacht.

Davon ausgehend nehmen wir im nächsten Teil die gängigsten Verfahren zur rechnergestützten Verschlüsselung näher unter die Lupe. Insbesondere wollen wir uns ansehen, für welche Einsatzgebiete RC4, MD5, DES, IDEA, RSA, Diffie-Hellman, SHA und DHA in Frage kommen, wie sicher sie sind, und welche Performance-Trade-offs man für die entsprechende Security in Kauf nehmen muss.

Axel Sikora

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Kryptographie-Grundlagen | a416 | – |
| Praxis der digitalen Signatur | a909 | – |
| Sicherheit im WLAN | a928 | – |
| Firewall-Grundlagen | a682 | – |
| Ausfallsichere Systeme | a422 | – |
| Sichere E-Mail | a398 | – |
| Lauschangriff im Firmennetz | a288 | – |

## 1.2 Kryptographische Verfahren

Verschlüsselungsverfahren kommt im Rahmen der Datenübertragung eine besondere Bedeutung zu. Die Kryptographie soll die Geheimhaltung von Daten ermöglichen. Schließlich hat jede Person und jede Organisation ein legitimes Interesse an dem Schutz seiner Daten vor Ausspähung, sei es im Bereich von vertraulichen Bank- und Börsengeschäften oder sei es die E-Mail mit der Einladung zu einem Bewerbungsgespräch, die der bisherige Arbeitgeber nicht zu Gesicht bekommen soll. Insbesondere Firmen sind darauf angewiesen, ihre Einkaufskonditionen oder ihre Forschungsergebnisse vor den Augen der Konkurrenz zu schützen.

Die berechnungssichere, so genannte starke Kryptographie zeichnet sich im Wesentlichen dadurch aus, dass ihre Algorithmen publiziert und allgemein bekannt sind. Die Entschlüsselung der verschlüsselten Nachricht ist dabei in vertretbarer Zeit ohne Kenntnis des Schlüssels nicht möglich. Die Publikation der Ver- und Entschlüsselungsalgorithmen ermöglicht es den Kryptoanalytikern in aller Welt, das Verfahren auf Herz und Nieren zu überprüfen. Nur ein Algorithmus, der seit einigen Jahren publiziert ist und untersucht wurde, kann als sicher gelten, sofern keine Schwachstellen gefunden wurden.

Grundsätzlich sind alle gängigen Kryptoalgorithmen durch Ausprobieren zu überwinden. Ob ein Kryptoalgorithmus sicher ist, hängt in der Praxis davon ab, ob der zum Knacken des Algorithmus notwendige Aufwand in Relation gesehen höher ist als der Wert der verschlüsselten Nachricht. Wenn das Ausprobieren selbst mit den schnellsten Computer weitaus länger dauert als die zu lesende Nachricht bedeutsam ist, kann von einem sicheren Algorithmus gesprochen werden. So ist zum Beispiel die Geheimhaltung der Konstruktionspläne eines neuen Autos spätestens nach dessen Markteinführung bedeutungslos. Ein Kryptoalgorithmus, bei dem das Entschlüsseln durch Ausprobieren mehr als zehn Jahre dauert, wäre in diesem Falle also sicher.

### 1.2.1 Symmetrische Verschlüsselungsverfahren

Exemplarisch für symmetrische Verschlüsselungsverfahren sehen wir uns drei Beispiele an: Die Verknüpfung mit Hilfe einer logischen Exklusiv-Oder-Funktion, den darauf aufbauenden RC-4-Algorithmus sowie den häufig verwendeten Data Encryption Standard (DES).

Der einfachste Einsatz symmetrischer Schlüssel basiert auf der logischen Exklusiv-Oder-Funktion. Die zweifache XOR-Verknüpfung eines Zeichens A mit einem Zeichen B hat wieder das ursprüngliche Zeichen A zum Ergebnis. Damit entspricht das zweifache Exklusiv-Oder mit einem identischen Zeichen also der inversen Verknüpfung.

Zur verschlüsselten Übertragung verknüpft der Sender ein Zeichen A mit einem Schlüssel B per XOR und übersendet dann das Resultat. Der Empfänger verknüpft das empfangene Zeichen erneut mit dem Schlüssel B und erhält dann das ursprüngliche Zeichen A.

### 1.2.2 RC-4

RC-4 wurde 1987 von dem bekannten Kryptographen Ron Rivest entwickelt. Das Kürzel RC steht für Rivest Cipher. Es handelt sich um ein einfaches und schnelles Stromverschlüsselungsverfahren, das auf der schon beschriebenen XOR-Verknüpfung basiert. Da sich der Algorithmus sehr gut zur Implementation in Software eignet, kam RC-4 schon bald in zahlreichen kommerziellen Produkten zum Einsatz, darunter Lotus Notes, Oracle Secure SQL und Netscape Navigator.

Die Stärke des Algorithmus besteht darin, dass mit einem einfachen Verfahren aus dem eingegebenen Schlüssel S ein langer, pseudo-zufälliger interner Schlüssel P erzeugt wird. Diesen nutzt RC-4 dann zur Chiffrierung des Klartexts. Besteht der Schlüssel S aus n Bytes von S(0) bis S(n-1), dann initialisiert man:

```
i, j = 0
P[k] = k mit k=0,...,256
```

und berechnet 256 Mal:

```
j = j+P[i]+S[i] mod 256
vertausche P[i] und P[j]
i = i+1 mod n
```

Das zur Ver- respektive Entschlüsselung des Nachrichten-Bytes i notwendige Schlüssel-Byte K[i] berechnet sich nach der Vorschrift:

```
i = i+1 mod 256
j = j+P[i] mod 256
vertausche P[i] und P[j]
t = P[i]+P[j] mod 256
K[i] = P[t]
```

Über die Variablen i und j sowie die Permutation P speichert RC-4 also 258 verschiedene Zustandsinformationen. 256 der Bytes sind Permutationen von 0, ...,255 und somit gleich verteilt.

## 1.2.3 DES

Der Data Encryption Standard (DES) wurde Mitte der 70er Jahre von IBM entwickelt, 1977 vom US-amerikanischen National Bureau of Standards vorgestellt und 1979 vom National Institute of Standards and Technology als Standard verabschiedet. DES gehört zur Familie der Blockchiffren und teilt eine Nachricht in 64 Bit große Datenblöcke auf. Auf der Verschlüsselungsseite umfasst es drei Bearbeitungsschritte, die wieder den Originaltext liefern, wenn man sie zur Entschlüsselung identisch durchführt.

DES zählt zu den heute immer noch am weitesten verbreiteten Verschlüsselungsalgorithmen. Zwar gilt der Ur-Algorithmus inzwischen nicht mehr als zeitgemäß. Die aktuelle Variante Triple-DES (3DES) jedoch führt die Verschlüsselung drei Mal hintereinander aus, was zu einer exponentiellen Steigerung der Sicherheit führt. 3DES findet vielfach Anwendung im Bereich der Finanzdienstleistungen.

## 1.2.4 Permutationen

DES besteht sowohl bei der Verschlüsselung als auch bei der Entschlüsselung aus den drei Bearbeitungsschritten initiale Permutation, Ver-/Entschlüsselung in mehreren Runden sowie finale Permutation.

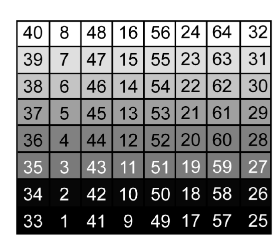
Initiale Permutation

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |

| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
|---|---|---|---|---|---|---|---|
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Finale Permutation

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
| 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |



| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
|---|---|---|---|---|---|---|---|
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |



**Bäumchen, wechsle dich:** In den Permutationsschritten kippt DES jeweils die Zeilen-/Spalten-Matrix der Bits.

$C_i$

| | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |

$D_i$

| | | | | | | |
|---|---|---|---|---|---|---|
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

$K_{il}$

| | | | | | |
|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |

$K_{ir}$

| | | | | | |
|---|---|---|---|---|---|
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |



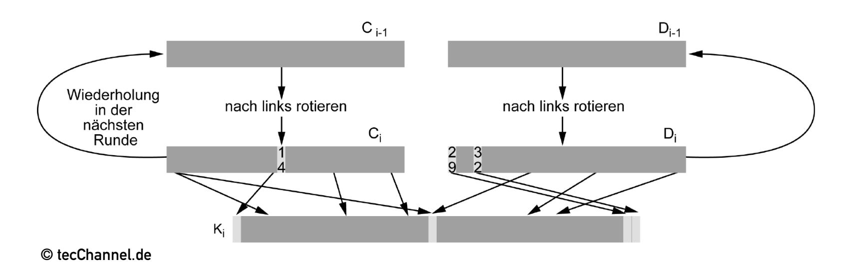
**Schlüsselpermutation bei DES**: Der Rundenschlüssel entsteht aus zwei je 28 Bit langen Teil-Keys.

Die Permutationen vor der ersten und nach der letzten Runde dienen keinerlei erkennbarem kryptologischen Zweck. Da DES ursprünglich zur Implementation in Hardware entwickelt wurde, vermutet man, dass die Umstellung der Bits zur Anpassung an die schmalen Register der 70er-Jahre-CPUs diente. Die finale Permutation bildet die Inverse der initialen Permutation, sie setzt die Bits also einfach wieder an die ursprüngliche Stelle.

## 1.2.5 Verschlüsselung

Die DES-Verschlüsselung basiert auf einem 64 Bit langen Schlüssel. Davon sind aber nur 56 Bit kryptographisch relevant, da es sich bei jedem achten Bit um ein Parity-Bit handelt. DES erzeugt aus diesen 64 Bit zunächst 16 verschiedene, jeweils 48 Bit lange Keys.

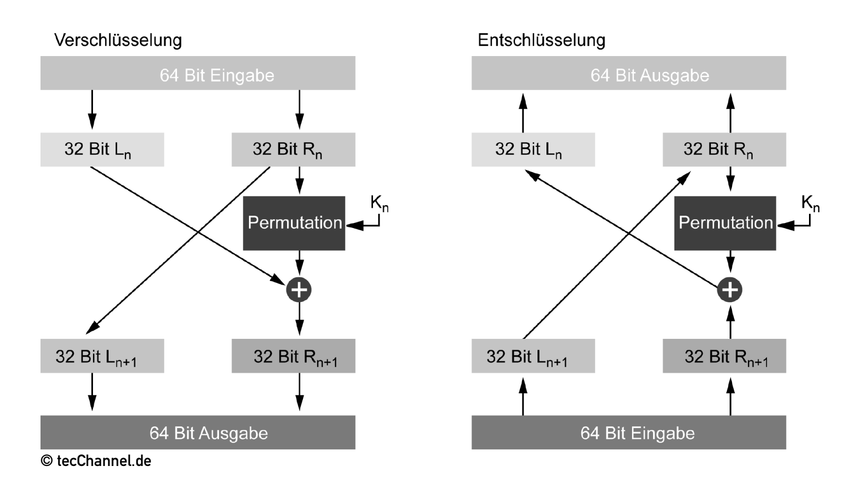
Dazu bildet es aus den 56 relevanten Bits mit Hilfe einer Permutation zwei 28 Bit lange Muster C[i-1] und D[i-1]. Anschließend rotiert DES diese beiden Teilschlüssel rundenabhängig um ein oder zwei Bit nach links. In den Phasen 1, 2, 9 und 16 wird um ein Bit geshiftet, in den anderen Runden um zwei Bit.




**DES-Schlüsseltransformation:** Sie sorgt für die Verwendung unterschiedlicher Schlüsselbits in jeder Runde.

Die so erzeugten Schlüssel C[i] und D[i] werden zu den neuen Schlüsseln C[i-1] und D[i-1]. Schließlich stellt eine weitere Permutation aus C[i] und D[i] zwei 24 Bit lange Folgen zusammen, die in Kombination zum Schlüssel K[n] werden.

Für die Verschlüsselung teilt DES den Klartext nun in jeweils 64 Bit lange Blöcke auf. Diese splittet es nochmals in zwei 32 Bit lange Bestandteile L[n] und R[n]. R[n] wird über eine so genannte Mangler-Funktion vermischt. Dazu kommt eine tabellenbasierte Umrechnung auf der Grundlage der Eingangsvariablen R[n] und des Schlüssels K[n] zum Einsatz.




**Blockbasiert:** DES verschlüsselt den Klartext in 64-Bit-Häppchen.

## 1.2.6 IDEA

Der International Data Encryption Algorithm (IDEA) wurde Anfang der Neunziger Jahre von Xuejia Lai und James Massey an der ETH Zürich (www.ethz.ch) entwickelt und 1991 veröffentlicht. Er zählt ebenfalls zu den Blockchiffren, wendet allerdings einen 128 Bit großen Schlüssel auf die 64 Bit langen Datenpakete des Klartextes an.

IDEA beruht auf der Mischung dreier mathematischer Funktionen, die jeweils auf 16-Bit-Blöcke des Textes angewendet werden. Neben der schon bekannten XOR-Funktion kommt eine Addition modulo $2^{16}$ zum Einsatz, die zwei Blöcke unter Verwerfen des Übertrags addiert.

Bei der dritten Funktion handelt es sich um eine Multiplikation modulo $2^{16}+1$, die zunächst zwei Blöcke multipliziert und das Resultat dann durch $2^{16}+1$ dividiert. Der Rest wird als 16-Bit-Ergebnis übernommen.

IDEA verknüpft diese drei Operationen zu einem recht komplizierten Netzwerk, das in insgesamt acht Runden durchlaufen wird. Trotz der komplizierteren Verfahrensweise operiert IDEA (als Software-Implementation) schneller als DES und gilt gleichzeitig als sicherer gegen Kryptangriffe.

### 1.2.7 Asymmetrische Verschlüsselungsverfahren

Während symmetrische Verfahren mit einem identischen Key zur Ver- und Entschlüsselung arbeiten, setzen die auch als Public-Key-Verfahren bezeichneten asymmetrischen Methoden auf zwei unterschiedliche Schlüssel.

Der eine Schlüssel heißt privater Schlüssel (Private Key), der zugehörige Algorithmus Dechiffrier-Algorithmus. Den anderen Schlüssel nennt man öffentlichen Schlüssel (Public Key), den entsprechenden Algorithmus Chiffrier-Algorithmus. Dabei lässt sich aus dem Public Key nicht auf den Private Key schließen. Daher kann man den Private Key ohne Gefahr öffentlich bekannt machen. Er ist von Dritten zur Verschlüsselung von Nachrichten nutzbar, die anschließend nur der Besitzer des zugehörigen Private Key wieder dechiffrieren kann.

Bekanntester Vertreter der Public-Key-Verfahren ist der nach den Initialen seiner Entwickler Ron Rivest, Adi Shamir und Leonard Adleman benannte RSA-Algorithmus. Er basiert auf der Grundlage, dass die Multiplikation zweier Zahlen eine einfache Operation darstellt, während der umgekehrte Vorgang, also die Faktorzerlegung eines Produkts, einen enormen Rechenaufwand bedeutet. Dies gilt insbesondere dann, wenn das Produkt in seine Primfaktoren zerlegt werden muss.

### 1.2.8 RSA

Der RSA-Algorithmus basiert auf folgenden vier Schritten:

- Wähle zwei große Primzahlen p und q, die geheim bleiben.
- Berechne das Produkt n = p*q. n wird als Modulus bezeichnet.
- Um einen öffentlichen Schlüssel zu erzeugen, wähle eine Zahl e kleiner n, die teilerfremd zur Eulerschen Funktion E(n) = (p-1)*(q-1) ist. Das bedeutet, dass e und E(n) keinen gemeinsamen Teiler außer 1 besitzen. [e,n] ist der öffentliche Schlüssel.
- Um den privaten Schlüssel zu erzeugen, bestimme eine Zahl $d = e^{-1}$ mod E(n). Dann gilt: e*d = 1 mod E(n). [d,n] ist der private Schlüssel.

Bei der Verschlüsselung kommt der RSA-Algorithmus wie folgt zum Einsatz:

- Alice verschlüsselt ihren Klartext m gemäß $c = m^e$ mod n und sendet ihn an Bob. In diesem Fall ist [e,n] der öffentliche Schlüssel von Bob.
- Bob entschlüsselt den Geheimtext c mit seinem privaten Key [d,n] gemäß m = $c^d$ mod n und erhält wegen des Zusammenhangs von d und e den Klartext m.

Wie man sieht, führt der Empfänger bei der Entschlüsselung die gleiche Operation durch wie der Sender bei der Verschlüsselung. In ähnlicher Weise lässt sich der RSA-Algorithmus zur Erzeugung und Überprüfung von Signaturen einsetzen:

- Alice sendet eine signierte Nachricht, indem sie $s = m^d \bmod n$ erzeugt und überträgt. [d,n] ist in diesem Fall der private Schlüssel von Alice.
- Bob entschlüsselt die Signatur gemäß $m = s^e \bmod n$ und erhält auf Grund des Zusammenhangs von d und e den Klartext m. [e,n] ist in diesem Fall der öffentliche Schlüssel von Alice. So kann jeder überprüfen, dass nur Alice die Signatur erzeugt hat.

## 1.2.9 Diffie-Hellman

Der nach seinen Erfindern benannte Diffie-Hellman-Algorithmus (DH) dient der Vereinbarung eines gemeinsamen symmetrischen Schlüssels über einen unsicheren Kanal. Wie RSA basiert DH auf einem öffentlichen und einem privaten Key:

- Beiden an der sicheren Kommunikation beteiligten Partnern Alice und Bob sind eine große Primzahl p und ein ganzzahliger Wert g (Generator) frei zugänglich.
- Alice generiert eine große Zufallszahl a, berechnet eine Zahl $A = g^a \bmod p$.
- Bob generiert ebenfalls eine große Zufallszahl b, berechnet eine Zahl $B = g^b \bmod p$ und sendet B an Alice.
- Alice berechnet eine Zahl $K[1] = B^a \bmod p$.
- Bob berechnet eine Zahl $K[2] = A^b \bmod p$.

Beide Zahlen K[1] und K[2] sind gleich, es gilt: $K = K[1] = K[2] = g^{a*b} \bmod p$. K wird nun als geheimer symmetrischer Schlüssel verwendet, der ohne Kenntnis von a und b nicht berechnet werden kann.

## 1.2.10 Man in the Middle

Der grundlegende Diffie-Hellman-Algorithmus gibt lediglich Sicherheit gegen passives Abhören. Ein Man-in-the-Middle-Angriff kann hingegen sowohl Alice als auch Bob suggerieren, dass nur sie miteinander sprächen. Ein solcher Angriff könnte folgendermaßen verlaufen:

- Die beiden Zahlen p und g sind nicht nur Alice und Bob, sondern auch dem Angreifer Mallory frei zugänglich.
- Alice versendet die Zahl $A=g^a \bmod p$. Mallory empfängt A, sendet aber $M = g^m \bmod p$ an Bob weiter.
- Bob versendet die Zahl $B = g^b \bmod p$. Mallory empfängt B, sendet aber $M = g^m \bmod p$ an Alice weiter.
- Alice berechnet nun ihre Zahl $K[1] = M^a \bmod p$. Mallory kann diesen Schlüssel ebenfalls durch $K[1m] = K[1] = A^m \bmod p$ berechnen.

- Bob berechnet eine Zahl K[2] = $M^b$ mod p. Mallory kann auch diesen Schlüssel durch K[2m] = K[2] = $B^m$ mod p berechnen.

Mallory kann nun alle Nachrichten von Alice an Bob aufnehmen, mit K[1m] entschlüsseln, mit K[2m] erneut verschlüsseln und dann an Bob weiterleiten. Gleiches tut er umgekehrt mit den Nachrichten von Bob an Alice. Sowohl Alice als auch Bob glauben, unmittelbar miteinander zu kommunizieren.

Das funktioniert aber nur, wenn Mallory die Möglichkeit hat, bei der Verteilung des öffentlichen Schlüssels eine Manipulation vorzunehmen. Wird der öffentliche Schlüssel authentifiziert oder über ein zuverlässiges Medium übertragen, dann ist der Diffie-Hellman-Algorithmus gegen solche Angriffe geschützt.

### 1.2.11 Einweg-Hash-Funktionen

Hash-Funktionen sind in der Informatik seit langem bekannt. Sie dienen beispielsweise bei Datenbank-Anwendungen zur einfachen Indizierung und somit dem schnellen Wiederauffinden von Informationen.

Dazu fassen sie umfangreiche Informationen – wie etwa Kundennamen oder Artikelbezeichnungen – durch Bilden irgendeiner Art von Quersumme zu einer komprimierten, leichter verwaltbaren Information zusammen. Letztere nennt man den Hash-Wert der Information. Die verwendete Hash-Funktion muss natürlich sicherstellen, dass für verschiedene Eingangsinformationen auch hinreichend unterschiedliche Hash-Werte entstehen.

Solche Hashes lassen sich auch gut zur Authentifizierung und Signatur einsetzen, falls der verwendete Algorithmus zwei zusätzliche Kriterien erfüllen kann. Zum einen darf es nicht möglich sein, mit vertretbarem Aufwand aus dem Hash-Wert die Originalinformation zu rekonstruieren. Zum anderen muss es aus Gründen der Fälschungssicherheit ausgeschlossen sein, mit vertretbarem Aufwand aus einer gegebenen Originalinformation eine zweite Information zu generieren, die denselben Hash-Wert ergäbe („Kollision“).

Einweg-Hash-Funktionen werden unter anderem auch als Kompressionsfunktion, Message Digest, kryptographische Prüfsumme oder Message Integrity Check (MIC) bezeichnet. Schon daraus lässt sich das breite Einsatzspektrum ersehen.

Da Einweg-Hash-Funktionen für jedermann berechenbar sein sollen, verwenden sie keine geheimen Schlüssel. Den Hash-Wert einer Einweg-Funktion bezeichnet man als Message Authentication Code (MAC).

### 1.2.12 MD-5

Zu den am weitesten verbreiteten Message-Digest-Funktionen zählt MD-5. Es gehört mit MD-2 und MD-4 zu einer Familie stetig verbesserter Hash-Funktionen, die von dem bereits mehrfach zitierten Ron Rivest entwickelt wurden.

MD-5 verarbeitet Nachrichten in 512-Bit-Blöcken, indem es jeweils sechzehn 32-Bit-Blöcke zusammenfasst. Auf Grund dieser Eigenschaft eignet sich MD-5 besonders für den Einsatz auf 32-Bit-Prozessoren. Auch als MAC erhält man einen 128 Bit langen Block aus vier 32-Bit-Blöcken.

Die Verarbeitung findet bei MD-5 in mehreren Stufen statt, wobei als Eingangsfolge jeder Stufe ein 512 Bit langer Block der Nachricht und das MAC der vorangegangenen Stufe dienen. Für die erste Stufe wird ein initialer MAC mit den vier 32-Bit-Blöcken d0 = 6745230116, d1 = efcdab8916, d2 = 98badcfe16 und d3 = 1032547616 verwendet. Beim MAC der letzten Stufe handelt es sich dann um den gültigen Message Digest.

## 1.2.13 SHA-1

Zu den Schwächen des MD-5-Algorithmus zählt, dass sich entgegen der Anforderung an Einweg-Hash-Funktionen relativ schnell Kollisionen der Hash-Werte ergeben können. Diesem Umstand versucht der 1994 von NIST (www.nist.gov) vorgeschlagene Secure Hash Algorithm SHA-1 abzuhelfen.

SHA-1 generiert aus einer maximal $2^{64}$ Bit langen Eingangsfolge eine 160 Bit lange Zeichenfolge. Dabei arbeitet es mit 512-Bit-Blöcken. Der Algorithmus verwendet fünf Stufen, wobei auf jeder Stufe 80 Schritte ausgeführt werden. Wie MD-5 nutzt auch SHA-1 anfangs einen vorgegebenen, initialen Message Digest.

Auf Grund seiner längeren Ergebnisfolge besteht bei SHA-1 eine wesentlich geringere Wahrscheinlichkeit für eine Kollision als bei MD-5. Während bei MD-5 durchschnittlich nach $2^{64}$ Operationen eine Kollision entsteht, ist dies bei SHA-1 erst alle $2^{80}$ Operationen der Fall.

## 1.2.14 DSA

Aus dem mittels einer Hash-Funktion generierten Message Authentication Code lässt sich eine digitale Unterschrift erzeugen, indem man ihn mit einem privaten Schlüssel chiffriert. Auf diesem Weg arbeitet etwa der Digital Signature Algorithm (DSA) des Digital Signature Standard (DSS, www.itl.nist.gov/fipspubs/fip186.htm). Er zeigt ein mögliches Vorgehen auf der Basis eines mit SHA-1 erzeugten MAC:

- Es wird eine große Primzahl p ausgewählt, die typisch zwischen 512 und 1024 Bits lang ist.
- Es wird ein Primfaktor q der Zahl (p-1) berechnet. q ist 160 Bits lang.
- Es wird eine Zahl g berechnet mit $g = h^{(p-1/q)} \bmod p$, wobei $h < p$ und $g > 1$.
- Es wird eine Zahl $x < q$ als privater Schlüssel des Senders Alice ausgewählt.
- Die Zahl $y = g^x \bmod p$ wird nun als öffentlicher Schlüssel verwendet.

- Alice unterzeichnet jetzt ihre Mitteilung an Bob mit $r = (g^k \bmod p) \bmod q$ sowie $s = (k^{-1}*(SHA1(m)+x*r)) \bmod q$.

Alice versendet nun (m, r, s). Der Empfänger Bob überprüft die digitale Unterschrift mit Hilfe von:

- $w = s^{-1} \bmod q$
- $u(1) = (SHA1(m)*w) \bmod q$
- $u(2) = (r*w) \bmod q$
- $v = ((g^{u(1)}*g^{u(2)}) \bmod p) \bmod q$

Falls v = r ist, gilt die Unterschrift von Alice als bestätigt.

Axel Sikora

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Kryptographie im Überblick (Teil 1) | a1068 | S.12 |
| Kryptographie-Grundlagen | a416 | – |
| Praxis der digitalen Signatur | a909 | – |
| Sicherheit im WLAN | a928 | – |
| Sichere E-Mail | a398 | – |
| Lauschangriff im Firmennetz | a288 | – |

# 1.3 Public-Key-Infrastrukturen

Sicherheitsmechanismen auf Basis von Public-Key-Systemen spielen zunehmend eine zentrale Rolle in Unternehmen. Doch stellt sich die Frage: Wie integriert man eine PKI effektiv in die bestehende IT-Landschaft.

Papier und „Snail-Mail“ sind out, elektronische Dokumente und E-Mail in. Während in der Vergangenheit die meisten Geschäftsprozesse persönlich oder papiergebunden abgewickelt wurden, können heute solche Abläufe durch eine globale IT-Infrastruktur weitaus rationeller gestaltet werden. Mehr und mehr werden in Wirtschaft, Industrie und Behörden deshalb Dokumente PC-basiert erfasst und über interne und externe Netze ausgetauscht. Der Vorteil: Die elektronischen Daten können direkt und ohne Medienbruch in die Arbeitsprozesse einbezogen werden. Die Folge ist eine immense Zeit- und Kostenersparnis.

Die verarbeiteten oder generierten Daten stellen einen wesentlichen Unternehmenswert dar. Der Schutz sensibler Firmendaten sollte deshalb oberste Priorität haben, Sicherheitsmaßnahmen sind unabdingbar. Denn für potenzielle Angreifer besteht jederzeit die Möglichkeit, Informationen aus einem öffentlichen Netz abzuhören, diese auszuwerten und zum Schaden des Unternehmens zu manipulieren. Schon mit einfachsten Mitteln bekommen nicht autorisierte Personen Zugriff zu sensiblen Informationen oder können etwa Mails von Dritten lesen und verändern.

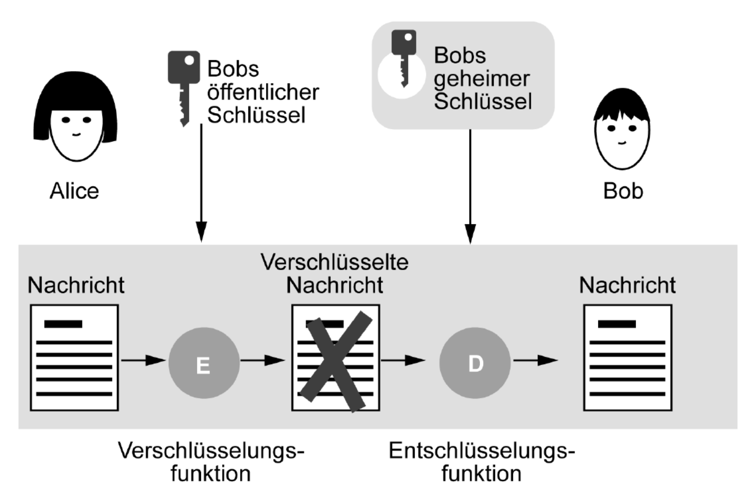
Vertraulichkeit, Authentizität und Integrität sind die Schlüsselkriterien zum Schutz der Anwendungen und Daten. Für diese Aufgabe haben sich in den letzten Jahren Sicherheitsmechanismen auf der Basis asymmetrischer Public-Key-Systeme durchgesetzt. Anwendern und Diensten kann damit eine netzweit verifizierbare Identität zugeordnet werden.

Dieser Beitrag klärt zunächst die grundlegenden Fragen, die bei der Planung einer Publik-Key-Infrastruktur (PKI) anstehen. Im zweiten Teil erfahren Sie dann mehr zu konkreten Anbietern und Lösungen.

## 1.3.1 Teil I: Public-Key-Infrastrukturen

Public-Key-Systeme helfen, eine geeignete Sicherheitsbasis zu schaffen. Der Einsatz von Public-Key-Kryptographie in Unternehmensnetzen setzt allerdings den Aufbau und Betrieb einer entsprechenden Infrastruktur voraus. Die Public-Key-Infrastruktur (PKI) ermöglicht es zum Beispiel, private Schlüssel sicher abzulegen, öffentliche Schlüssel in allgemein zugänglichen Verzeichnissen zu organisieren und Soft- und Hardware-Module bereitzustellen, mit denen man verschlüsseln und signieren kann.

Eine funktionierende PKI verhindert dann, dass sich jemand unter einer falschen Identität an der Kommunikation beteiligt oder dass jemand ein Dokument liest, für den es nicht bestimmt war.




**Getrennt:** Beim Verfahren mit Public Keys kommen ein öffentlicher und ein geheimer Schlüssel zum Schutz der Nachricht zum Einsatz.

Allgemein besteht eine PKI aus Hardware, Software und abgestimmten, unternehmensweiten Richtlinien, der Policy. Die Policy definiert, nach welchen Sicherheitsregeln die Dienstleistungen erbracht werden. Dazu zählt das Betriebskonzept der PKI, die Benutzerrichtlinien sowie Organisations- und Arbeitsanweisungen.

## 1.3.2 Digitales Zertifikat

Das zentrale Element der PK-Struktur ist der digitale Ausweis, das Zertifikat. Das Zertifikat ist quasi der Pass oder Personalausweis, der den Inhaber im elektronischen Geschäftsverkehr identifiziert. Es enthält Informationen zum Zertifikatsinhaber, zum Zertifikatsaussteller und dient der Zuordnung eines Schlüsselpaares zu einer Person.

Wichtigster Bestandteil des Zertifikats ist der öffentliche Schlüssel des Inhabers, der untrennbar mit dem Inhaber verbunden ist. Mit diesem Schlüssel ist es jedermann möglich, die elektronischen Signaturen des Zertifikatsinhabers zu prüfen. Darüber hinaus trägt das Zertifikat eine eindeutige Nummer, es enthält den Namen des Besitzers und ein Gültigkeitsdatum, das angibt, wann das Zertifikat abläuft. Die folgende Tabelle zeigt die wichtigsten Analogien und Gemeinsamkeiten zwischen Personalausweis und digitalem Zertifikat.

| **Analogien Personalausweis und digitales Zertifikat** | |
|---|---|
| **Personalausweis** | **Digitales Zertifikat** |
| Vor- und Nachname des Eigentümers | Name oder Pseudonym des Eigentümers |
| Ausstellende Behörde | Zertifizierungsstelle (Trustcenter) |
| Ausstellungsdatum | Ausstellungsdatum |
| Gültigkeitsdauer | Gültigkeitsdauer |
| Identifizierungsnummer | Identifizierungsnummer |
| Eigenhändige Unterschrift | Privater und öffentlicher Schlüssel |

Als Trägermedium für die Zertifikate kommen – neben passwortgeschützten Dateien und USB-Token – vor allem Smartcards zum Einsatz. Diese enthalten einen miniaturisierten Chip, der die Public-Key-Algorithmen und Daten speichert. Der Vorteil: Da die Verschlüsselung auf der Karte erfolgt, muss der private Schlüssel nie die Karte verlassen. Dies bietet einen deutlichen Sicherheitsvorteil gegenüber reinen Software-Lösungen.

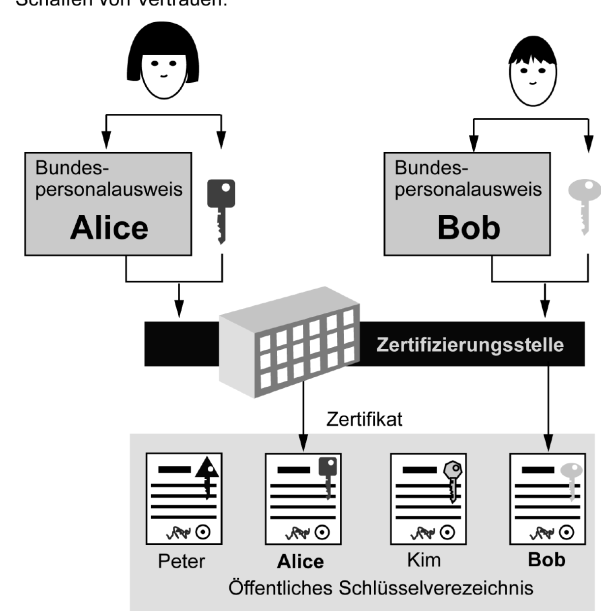



**Doppelter Schutz:** Die Smartcard wird zum elektronischen Signieren in ein Kartenlesegerät geführt und die Aktion mit der Eingabe eines PIN-Codes bestätigt. (Quelle: Utimaco Safeware)

Außerdem ist die Benutzung der Karte erst nach Eingabe einer schützenden PIN-Nummer möglich. Und nicht zuletzt schreibt das deutsche Signaturgesetz die Verwendung von Chipkarten bei gesetzeskonformen Anwendungen zur digitalen Signatur explizit vor.

## 1.3.3 Trustcenter

Damit niemand ein Zertifikat manipulieren und man sicher sein kann, dass alle Angaben korrekt sind, braucht man eine „Meldebehörde“, die das Zertifikat ausstellt und „versiegelt“. Diese Aufgabe übernimmt die Zertifizierungsstelle, im Fachjargon Trustcenter oder Certification Authority (CA) genannt. Sie stellt die zentrale Institution des Vertrauens dar, indem sie eine verbindliche dezidierte Zuordnung von Schlüsselpaaren zu Personen vornimmt („Zertifizierung“). Die CA vergibt eindeutige Identitäten und verwaltet für jeden Teilnehmer ein Schlüsselpaar mit dem dazugehörigen Zertifikat. Jedes von der CA erzeugte Zertifikat verbindet den öffentlichen Schlüssel des Teilnehmers mit dessen Namen und den oben genannten zusätzlichen Daten. Auf diese Weise bürgt die CA dafür, dass der Name und der öffentliche Schlüssel im Zertifikat zu derselben Person gehören.





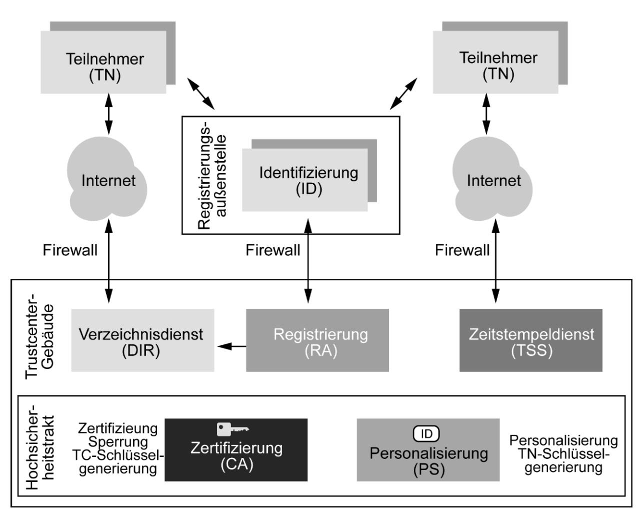

**Öffentlich:** Zertifizierungsstellen (CAs) stellen Zertifikate aus, die die Identität des Teilnehmers unmittelbar mit dem korrespondierenden öffentlichen Schlüssel verknüpfen und veröffentlichen dieses in einem allgemein zugänglichen Verzeichnis.

Im Allgemeinen ist es üblich, die Registrierung der Teilnehmer und die Zertifizierung der Schlüssel voneinander zu trennen und zum Teil auch an unterschiedlichen Orten vorzunehmen. Die CA nimmt dann reine Zertifizierungsaufgaben wahr, die Benutzeranfragen zur Zertifizierung werden hingegen von einer eigenen Institution erfasst, der Registration Authority (RA).

Die RA kümmert sich darum, dass der Anwender sich ordnungsgemäß nach den Richtlinien der Policy bei der Registrierung identifiziert. Sie leitet den Antrag auf Ausstellung eines Zertifikates an die entsprechende CA weiter und verwaltet die ausgestellten Benutzerzertifikate.

## 1.3.4 Die Dienste der CA und RA im Überblick

Die zertifizierten öffentlichen Schlüssel müssen schließlich auch veröffentlicht werden. Dies erfolgt für gewöhnlich in einem LDAP-Verzeichnisdienst (Directory Service, LDAP: siehe Glossar). Ein Verzeichnisdienst ist eine Art „Telefonbuch", das die Namen der Anwender und – anstelle der Telefonnummer – die dazugehörigen öffentlichen Schlüssel enthält. Hier kann der Empfänger einer signierten Nachricht den aktuellen Status eines Zertifikats nachschlagen.




**Vielfältig:** Die Dienste der CA und RA im Überblick.

Über den Verzeichnisdienst werden auch Sperrlisten („Certificate Revocation List", CRL) zur Verfügung gestellt, das sind Zertifikate, die während ihrer Gültigkeitsperiode von der CA für ungültig erklärt wurden. Gründe können sein: Be-

kanntwerden des Passworts, Missbrauch des Zertifikats, oder der Zertifikatsbesitzer verlässt die Firma, die das Zertifikat ausgestellt hat. Ein Zeitstempeldienst dient dazu, gesicherte Zeitsignaturen zu erstellen und ein Dokument oder eine Transaktion mit der aktuellen Zeitangabe zu verknüpfen.

Der Vorteil eines Zeitstempels, wie ihn TC TrustCenter mit „TC TimeStamp" liefert, ist nicht nur der Beweis, dass die elektronischen Daten zu einem bestimmten Zeitpunkt vorgelegen haben. Vielmehr wird auch jede nachträgliche Änderung erkennbar gemacht.

### 1.3.5 PKI Enabled Applications

Schließlich gehören zur PKI auch die Anwendungen, die auf der Grundlage der von der PKI zur Verfügung gestellten Sicherheitsdienste (Zertifikate, Verzeichnisdienst et cetera) eine vertrauenswürdige Nutzung ermöglichen, die „PKI-enabled Applications" (PKA). Typische PKI-Anwendungen sind:

- Sichere E-Mail-Anwendungen – der Inhalt kann verschlüsselt/entschlüsselt und digital unterschrieben werden;
- Sichere Desktop-Anwendungen – Office-Applikationen können durch Schaffung authentifizierter Systemzugänge beziehungsweise -sperren effizient abgesichert und verschlüsselt/entschlüsselt werden;
- Identifikations- und Authentisierungsprozesse, etwa an Netzen, so dass nur berechtigten Personen Zutritt gewährt wird;
- die Verschlüsselung von Datenverkehr beim Remote Access;
- Sichere Zugangskontrollen – diese sichern nur authorisierten Personen Zugriff zu sensiblen Informationen;
- Absicherung webbasierter Anwendungen – Der Zugang zu Internet-Seiten lässt sich mit Hilfe authentifizierter Zugangskontrollen vor unerwünschten Zugriffen absichern;
- Virtuelle Private Netzwerke (VPNs) – diese werden von Firmen zur sicheren Kommunikation über unsichere Netze (etwa das Internet) verwendet – durch die Schaffung verschlüsselter und authentifizierter Kommunikationskanäle.

Damit dürfte klar sein, dass es sich bei PKI um mehr als nur eine Kryptographielösung handelt. Zwar ist die Kombination aus öffentlichem und privatem Schlüssel die Grundlage, doch integriert eine derartige Kryptographielandschaft wesentlich vielfältigere Services, die vor allem das Management von Schlüsseln und Zertifikaten betreffen. Erst das einwandfreie Zusammenspiel aller Komponenten wie Certification Authority, Registrierungsstellen und Verzeichnisdienst garantiert die unternehmensweite Sicherheit.

## 1.3.6 Integration einer PKI in die Firmenstruktur

Die Einführung von PKI stellt Firmen vor eine ganze Reihe gravierender Probleme. PKI-Consultants haben die Erfahrung gemacht, dass Unternehmen oft zu kurzfristig und unangemessen an die Einführung von PK-Infrastrukturen herangehen. Viele betrachten PKI als notwendiges Übel und installieren gleich bestimmte Software-Produkte. PKI ist jedoch nicht als Ansammlung von Software zu verstehen, sondern als Sicherheitskonzeption. Am Anfang steht deshalb ein grundlegendes PKI-Konzept.

Oberstes Ziel einer PKI sollte sein, die im Unternehmen übliche Vielfalt an Sicherheits- und Kryptographieverfahren zu beseitigen und zu vereinheitlichen. Bislang existieren in den meisten Firmen getrennte und redundante Sicherheitslösungen, etwa für die Anmeldung am Netzwerk, das Abrufen von E-Mails oder den Remote-Access-Zugang.

Dies kostet Zeit und Geld und ist fehleranfällig. Mit einer funktionierenden PKI hingegen gibt es nur noch eine vertrauenswürdige Netzwerkumgebung, in die sich die verschiedenen Anwendungen einbetten lassen. Anstelle von Passwörtern können sich Anwender mit Hilfe ihrer geheimen Schlüssel und ihrer Zertifikate am Netzwerk oder an Servern anmelden. E-Mails können mit den Schlüsseln und Zertifikaten verschlüsselt oder digital unterschrieben werden.

Die PKI kann die Schlüssel für große VPNs oder die Kunden und Partner in einem E-Business-Projekt verwalten. Sogar die Zugangskontrolle für Räume lässt sich in die PKI einbinden. Anstelle von separaten Verwaltungssystemen, in denen der Benutzer mehrfach redundant gepflegt werden muss, vereinigt die PKI also die Administration.

Für die konkrete Planung einer PKI gibt es kein allgemeingültiges Konzept. Es gibt jedoch ein Reihe von zu beantwortenden Fragen und Schritten, die möglichst eingehalten werden sollen. Grundlage der Planung sind Fragen wie:

- Sollen grundsätzlich externe Dienstleister eingeschaltet werden und wenn ja, in welchem Umfang?
- Welche Daten und Anwendungen sollen geschützt werden (E-Mail, VPN, Dateiverschlüsselung, Authentisierung, elektronische Rechnungen, ...)?
- Sollen Soft-Token oder Smartcards zur Speicherung der Zertifikate verwendet werden?
- Welcher Level der Gesetzeskonformität soll erfüllt werden?
- Soll Interoperabilität zu anderen PK-Strukturen und Anwendungen bestehen?
- Wie werden die Nutzer die PKI akzeptieren? Welche Kosten werden entstehen?

### 1.3.7 Stufenmodell

Der Aufbau einer eigenen PKI sollte in jedem Fall erst konzipiert und dann in einem Pilotprojekt getestet werden. Der Hamburger PKI-Dienstleister TC Trustcenter schlägt ein vierstufiges Vorgehen vor. In der ersten Phase wird gemeinsam mit dem Kunden abgeklärt, wofür die PKI genutzt werden soll, wie die Antragswege aussehen und auf welchem Speichermedium die Zertifikate ausgeliefert werden sollen. Die zweite Phase ist die konkrete Einrichtung der PKI entsprechend den Kundenwünschen. In der dritten Phase wird die PKI beim Kunden im Pilotbetrieb getestet, bevor sie letztlich mit der vierten Phase „in Produktion geht".

Der Münchner PKI-Dienstleister Integralis nutzt ebenfalls ein mehrstufiges Entwicklungskonzept. Im optimalen Fall sollte die Planung und Vorbereitung eines PKI-Projekts nach Auffassung der Integralis-Spezialisten etwa zehn Prozent der Kosten/Ressourcen des Gesamtumfangs betragen. Prinzipiell kann man ein solches Projekt in sieben Phasen untergliedern:

- Schritt 1: Bedarfsanalyse
- Schritt 2: Definition der Architektur
- Schritt 3: Betriebskonzept
- Schritt 4: Risikoanalyse
- Schritt 5: Pilotphase
- Schritt 6: Integration
- Schritt 7: Kontinuierliche Anpassungen

Schritt 1 definiert die Anforderungen, die an das PK-System gestellt werden. Dazu gehören Forderungen rechtlicher Art, die Frage, welche Daten und Anwendungen eingebunden sein sollen und betriebliche Erfordernisse wie Bandbreiten oder Verfügbarkeit. Schritt 2 beantwortet Fragen wie: Welche Systeme müssen integriert und abgesichert werden? Wie sieht die Gesamtarchitektur aus? Welche Teststrategie gibt es? Wie sieht der Projektplan aus? Schritt 3 legt fest, wie der Betrieb organisiert wird, wie die Handbücher und Anweisungen aussehen sollen, wie das Notfallmanagement gestaltet wird oder die Wartung organisiert ist. Bei der Risikoanalyse in Schritt 4 werden alle existierenden Werte, die Bedrohungen und Schwachstellen sowie geplante und existierende Sicherheitsmaßnahmen abgewogen, und eine finale Entscheidung für die Implementierung wird getroffen. Anschließend in Schritt 5 wird die PKI getestet und in Betrieb genommen. Bestehende Anwendungen werden integriert und die PKI kontinuierlich an neue betriebliche Erfordernisse angepasst.

Die erfolgreiche Planung einer größeren PKI ist in jedem Fall ein komplexes Unternehmen, für die externe Beratung dringend anzuraten ist. Security- und PKI-Consultants wie Secude, Utimaco (www.utimaco.de) oder Integralis (www.integralis.de) stehen mit fachmännischem Know-how zur Seite bzw. übernehmen komplett die Planung und Umsetzung.

## 1.3.8 Trustcenter-Betrieb – intern oder extern?

Eine Schlüsselfrage, die sich jedem Unternehmen bei der Einführung von PKI stellt, ist, ob ein eigenes Trustcenter betrieben werden soll oder ob externe Dienstleister in Anspruch genommen werden sollen. Gesetzlich sind in Deutschland zwei Typen von Zertifizierungsdiensten zugelassen.

Bei einem angemeldeten Zertifizierungsdienst reicht eine Erklärung über die Sicherheit aus. Er ist nur bei den zuständigen Behörden gemeldet, aber keinerlei behördlicher Kontrolle unterworfen. Im Falle eines Rechtsstreits muss die Sicherheit vom Zertifikatnehmer – also dem Unternehmen – bewiesen werden.

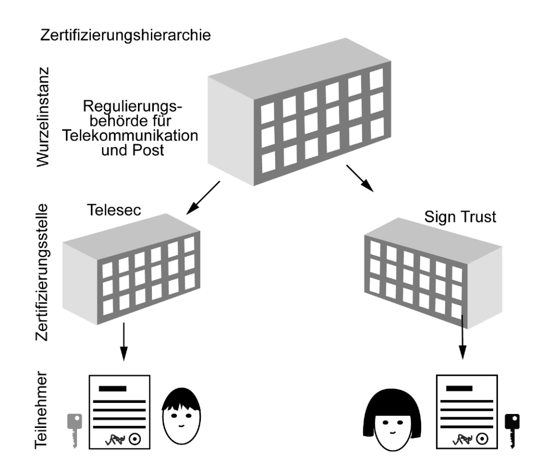
Im Gegensatz dazu überprüfen und bestätigen bei akkreditierten Zertifizierungsdiensten unabhängige Dritte die Sicherheit. Mit der Akkreditierung lässt sich die CA vorab von der Regulierungsbehörde für Telekommunikation und Post prüfen.

Der Aufbau einer unternehmenseigenen CA bedeutet einen enormen Zeit- und Kostenaufwand, insbesondere die Installation einer akkreditierten Zertifizierungsstelle ist kostspielig. Sie stellt besonders hohe Anforderungen an die bauliche Sicherheit, die Rechnerkapazitäten, die Zugriffssicherheit und die oben erwähnte gesamte Administration. Der Vorteil: In der Regel bietet ein selbst aufgebautes und betriebenes Trustcenter kürzere Reaktionszeiten, zum Beispiel beim Recovery, und ermöglicht eine größere Flexibilität. Dadurch wird der Ausfall bei Problemfällen minimiert, und im laufenden Betrieb lassen sich Kosten sparen.

## 1.3.9 Sinnvoll nur bei vielen Usern

Der Aufbau eines eigenen Trustcenters kann bei sehr speziellen Anforderungen an die PKI oder sehr großen Nutzerzahlen sinnvoll sein. Im Wesentlichen ist die Alternative Eigen- oder Fremdbetrieb aber eine Kosten- beziehungsweise Renditefrage und lohnt sich in der Regel nur für sehr große Unternehmen. Bei externem CA-Betrieb verteilen sich die Kosten auf regelmäßige Service-Zahlungen an den Dienstleister und die Anzahl der benötigten Zertifikate.

Aktuell sind allerdings nur wenige akkreditierte Trustcenter verfügbar. Allgemein zugängliche CAs, die Zertifikate anbieten, betreiben das TC Trustcenter (www.trustcenter.de) aus Hamburg, die Deutsche Post mit Signtrust (www.signtrust.de) und die Telekom-Tochter Telesec (www.telesec.de). Die anderen bisher akkreditierten Zertifizierungsstellen richten sich vornehmlich an geschlossene Benutzergruppen. So sind die Zertifikate der Datev eG nur für Steuerberater verfügbar. Eine Liste der akkreditierten Zertifizierungsdienste hat die zuständige Regulierungsbehörde für Telekommunikation und Post (RegTP) auf der Webseite www.regtp.de zusammengestellt.




© tecChannel.de

**Oberste Instanz der Hierarchie:** Die RegTP fungiert in Deutschland als Wurzelinstanz.

Jedes akkredidierte Trust Center benötigt einen übergeordneten vertrauenswürdigen Dritten, der ihm wiederum die Gültigkeit seines öffentlichen Schlüssels in einem Zertifikat bestätigt. Die Zertifikatkette kann je nach Sicherheitsinfrastruktur bis zu einer anerkannten Wurzelinstanz fortgesetzt werden. Der Schlüssel der obersten Instanz wird dann zwecks Authentizität auf konventionelle Art veröffentlicht, z.B. ist der öffentliche Schlüssel der RegTP, die in Deutschland als Wurzelinstanz fungiert, im Bundesanzeiger veröffentlicht.

## 1.3.10 Mischlösungen

Sourced man die Dienstleistung aus oder kauft sich diese Dienstleistung bei Dritten ein, so hat man allerdings auch diverse Risiken zu tragen: Ist der Dienstleister beispielsweise auch langfristig verfügbar, kann er bedarfsorientierte Reaktionszeiten garantieren? Integralis plädiert in der Frage Intern oder Extern für eine vernünftige Bedarfsanalyse. „Da müssen letztlich alle Kosten, insbesondere die operativen, ins Kalkül gezogen werden. Es gibt einige interessante Modellrechnungen, die besagen, dass das Outsourcing für kleinere Benutzerzahlen vorteilhafter ist. Irgendwo zwischen 10K und 50K Benutzern rentiert sich dann eine eigene PKI.“

Häufig werden auch Mischlösungen (Co-Sourcing) gewählt, bei denen Teile der Administration im Hause laufen und andere ausgelagert werden. Für qualitativ hochwertige Zertifikate, die z.B. unternehmensextern akzeptiert werden sollen, bedient man sich eines externen, etablierten Trustcenters am Markt. Für interne Anwendungen wie zum Beispiel Serverauthentifizierung werden hingegen eigenproduzierte Zertifikate verwendet – und zwar mit weit weniger hohen Sicherheitsanforderungen als gesetzlich verlangt. Für unternehmensinterne Zwecke genügt dies, der Vorteil liegt in der höheren Flexibilität – je nach Einsatzzweck das optimale Zertifikat – und in Kostenaspekten.

Ein zweigleisiges Vorgehen kann auch bei der Aufteilung in CA- und RA-Dienste sinnvoll sein. Zum Beispiel kann in einem Unternehmen der IT-Bereich die CA betreiben, während die Aufgaben einer Registrierungsstelle von der Personalabteilung übernommen werden. Bei internationalen Unternehmen mit mehreren Standorten kann es von Vorteil sein, wenn es eine einzige zentrale CA gibt, aber jeder Standort eine separate Registrierungsstelle besitzt, an die der Anwender sich direkt wenden kann.

## 1.3.11 Gesetzeskonform signieren – ja oder nein?

Eng mit dem Trustcenter verknüpft ist die Frage, welchen Anforderungen Signaturen in der Unternehmenspraxis genügen sollen. Der Gesetzgeber hat mit dem Signaturgesetz (SigG) zwar sichere und strenge Richtlinien vorgegeben, diese sind aber aufwendig zu realisieren. Damit stellt sich die Frage, welche Art von Signaturen in PKI-Umgebungen eingesetzt werden soll.

Gesetzlich gibt es grundsätzlich zwei verschiedene Signaturen: Einfache oder fortgeschrittene elektronische Signaturen bilden die „weichen“ Signaturen, die nach EU- und deutschem Recht der handschriftlichen Unterschrift nicht gleichgestellt sind. Solche Signaturen kann man zum Beispiel schon ganz einfach mit PGP (Pretty Good Privacy) erzeugen. Der handschriftlichen Unterschrift juristisch gleichgestellt ist erst die qualifizierte elektronische Signatur. Nur sie hat vor Gericht Beweiskraft und bildet praktisch den EU-Mindeststandard für Signaturen. Nur akkreditierte Trustcenter dürfen qualifizierte elektronische Signaturen ausstellen.

Im Unternehmensbereich sind qualifizierte Signaturen aufwendig und teuer zu realisieren. Viele Firmen verzichten daher auf die Umsetzung solcher Signaturen. Dies ist auch nicht notwendig. Denn bei qualifizierten Signaturen handelt es sich nur um ein Angebot. Wer sie nicht verwendet, verzichtet lediglich auf damit verbundene Rechtsfolgen. Allein in der Bundesrepublik gibt es mehrere 100.000 nicht qualifizierte Zertifikate, auf denen die Unternehmen trotzdem ihre Sicherheit – intern und zu Partnern – aufbauen. Das liegt daran, dass es den Unternehmen zuerst einmal auf die praktische Verwendbarkeit ankommt.

## 1.3.12 Weich reicht aus

Für die meisten PKI-Experten ist klar, dass qualifizierte Signaturen nach dem Signaturgesetz derzeit fast ausschließlich im sicherheitssensiblen Behörden- und Bankenbereich eine größere Rolle spielen. „In Unternehmen erfordern allenfalls bestimmte personenorientierte Verwaltungsprozesse qualifizierte Signaturen, die ein hohes Rationalisierungspotenzial erschließen, wie etwa der Vorsteuerabzug“, sagt Utimaco-Vorstand Norbert Pohlmann. Da in Unternehmen aber hauptsächlich bilaterale Beziehungen, etwa zum Hersteller oder Kunden, vorliegen, hat das Signaturgesetz dort auch schon aus diesem Grund relativ wenig Bedeutung.

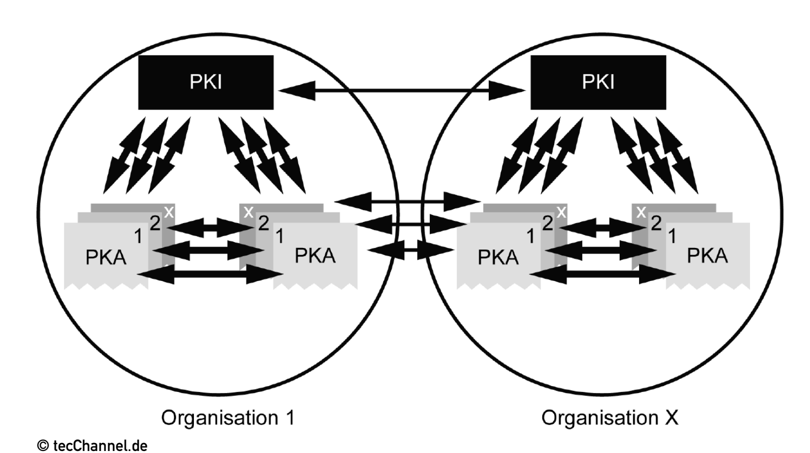
Für Anwendungen wie etwa die Signatur und Verschlüsselung von E-Mails sind die „weichen“ einfachen oder fortgeschrittenen Signaturen daher völlig ausreichend. Da hier wesentlich weniger Auflagen existieren, können diese häufig günstiger bereitgestellt werden. „In Unternehmen sind aber auch Mischformen sinnvoll“, betont Waltraud Tybussek von Telesec. „Es erhalten dann nur explizit die Mitarbeiter die Ausstattung für qualifizierte Signaturen, die diese für ihre speziellen Anwendungen benötigen.“

Allerdings kann in Zukunft die Bedeutung qualifizierter Signaturen zunehmen, wenn sich die Anwendungen in offene Bereiche bewegen, also unternehmensübergreifend eingesetzt werden. Da sich gesetzeskonforme Signaturen allgemeiner verwenden lassen, können sich mittelfristig stärkere Signaturen durchsetzen.

## 1.3.13 Offene Systeme für die Außenkommunikation

Bislang konzentrierten sich Unternehmen weit gehend auf die interne PKI, die vollständig in ihrem eigenen Verantwortungsbereich liegt. Sicherheitsdienste stehen nur innerhalb der Infrastruktur zur Verfügung, für die Kommunikation nach außen wird sie nicht genutzt. Da jedoch in der Praxis viele unternehmensübergreifende Prozesse stattfinden, ist der Nutzen einer solchen PKI sehr eingeschränkt.

Ökonomisch sinnvoll sind PKIs nur dann, wenn der Einsatz so umfassend wie möglich realisiert wird, d.h. wenn die gesicherte Kommunikation mit so vielen Partnern wie möglich stattfinden kann. Gegenwärtig verschiebt sich der Akzent deshalb auf offene PKI-Systeme. Dabei wird die PKI auch für die externe Kommunikation nach außen genutzt. Der Austausch beruht auf gegenseitigem Vertrauen sowie auf kompatiblen Technologien und Verfahren.




**Kommunikativ:** Offene PK-Systeme lassen sich für die Kommunikation mit anderen Unternehmen nutzen.

Bei offenen Systemen muss zum Aufbau einer organisationsübergreifenden Kommunikation ein Abgleich der verschiedenen organisationsspezifischen Policies erfolgen. Ziel ist ein gemeinsames „Level of Trust“. Hier müssen geeignete Instrumente implementiert werden, um die organisatorischen sowie die IT-infrastrukturellen Konzeptionen zu bewerten, zu analysieren und zu gewichten.

## 1.3.14 Traurige Realität

Die Realität ist leider, dass sich die beteiligten Unternehmen nur schwer auf den Abgleich ihrer individuellen Sicherheitskonzepte einigen können. Dadurch gestaltet sich der Aufbau eines gemeinsamen „Level of Trust“ langwierig, und längst fällige Entscheidungen werden nicht getroffen.

Die Bemühungen um Interoperabilität von PKI-Systemen werden durch die Vielfalt der Standards und ihrer Interpretationsmöglichkeiten erschwert. Zwei Lösungsansätze bieten sich derzeit an: Die ISIS-MTT und die Bridge-CA.

European Bridge-CA
Brücke des Vertrauens zwischen PKIs
Elektronischer Geschäftsverkehr
vertrauenswürdige Anwendungen
Authentisierung von Usern und Servern
Vertrauliche Kommunikation (SSL)
Dateiverschlüsselung
Verschlüsselte Email (S/MIME)
Datenauthentizität und -integrität (digitale Signatur)
Zeitstempeldienst
Virtual Private Network (VPN)
Single Sign On
weitere PKI-Dienste
ISIS-MTT
Spezifikation, Testkonzeption, Testbed
gemeinsame Grundlage für interoperable PKI-Systeme



**Vereinigung:** ISIS-MTT und die European Bridge-CA wollen PKIs miteinander verbinden.

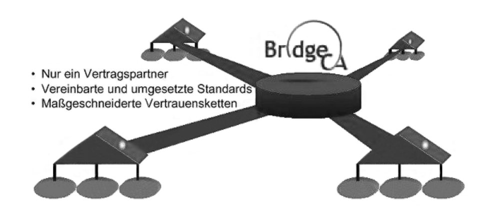
Um eine gemeinsame Grundlage zu schaffen, haben die Vereinigungen TeleTrusT e.V. und T7 e.V. mit Unterstützung durch das Bundeswirtschaftsministerium die Spezifikation ISIS-MTT ins Leben gerufen. Deren übergeordnetes Ziel ist eine schnelle flächendeckende Einführung PKI-gestützter Sicherheitstechnologie.

Die ISIS-MTT-Spezifikation basiert auf internationalen Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI etc.) und integriert die aus der bisherigen Anwendung gewonnenen Erfahrungen. Um die Voraussetzungen für die Entwicklung interoperabler Anwendungen auf internationaler Ebene zu schaffen, wird die Akzeptanz von ISIS-MTT in den europäischen und weltweiten Standardisierungsgremien angestrebt.

## 1.3.15 Europaweite Lösung

Die European Bridge-CA will das Interoperabilitätsproblem auf organisatorischer Ebene lösen. Sie hat sich das Ziel gesetzt, die Vertrauenslücken sowohl zwischen existierenden und noch einzurichtenden PKIs pragmatisch zu überbrücken. Die Bridge-CA-Initiative wurde von der Deutschen Bank und der Deutschen Telekom ins Leben gerufen und wird von der industriellen Vereinigung TeleTrusT Deutschland e.V. betrieben.

Das Ziel der europäischen Bridge-CA ist es, eine „Brücke des Vertrauens" zwischen verschiedenen PKIs weltweit herzustellen, indem sie minimale Policy-Anforderungen und technische Vorbedingungen definiert, die eine sichere Kommunikation über organisatorische Grenzen hinweg erlauben. Dabei wird auf bestehende Sicherheitstechnologie aufgesetzt, die getätigten Investitionen sind geschützt.




**Brücke des Vertrauens:** Die Bridge-CA verknüpft bestehende PK-Infrastrukturen.

Die Bridge-CA stellt eine allgemeine Plattform zur Verfügung, die die teilnehmenden CAs auf eine sichere, aber einfache Weise verbindet. Sie basiert auf einem standardisierten technischen und organisatorischen Regelwerk, das die Integration neuer CAs in die Bridge-CA-Infrastruktur erleichtert. Sobald ein neuer Teilnehmer sich anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner sicher kommunizieren.

Eine formale Prozedur für die Registrierung stellt sicher, dass alle Teilnehmer den Mindestanforderungen gerecht werden. Um einer breiten Klientel den einfachen und schnellen Zugang zu ermöglichen, wurden die Teilnahmevoraussetzungen minimal gehalten.

Die Bridge-CA bietet eine praktikable Lösung für das Verbinden voneinander unabhängiger PKIs. Nutzer dieser PKI können sicher und ohne größeren Aufwand miteinander kommunizieren. Letztes Jahr waren bereits 300.000 Zertifikate von Teilnehmern der Bridge-CA im Einsatz.

Der derzeitige Aufbau der European Bridge-CA ermöglicht es, zwischen den aktuellen vier aktiven PK-Infrastrukturen der Bundesverwaltung, der Deutschen Bank, der Deutschen Telekom und Siemens Daten auf sicherem Wege auszutauschen. Interessenten können sich direkt an die Bridge CA (www.bridge-ca.org) oder an Trustcenter (www.trustcenter.de) wenden.

### 1.3.16 Fazit

Der Aufbau einer PKI ist ein komplexes Unterfangen, das sorgfältig geplant werden sollte. Eine unternehmensweite, sichere zertifikatsbasierte Kryptographie-Infrastruktur aufzubauen, erfordert genaueste Analysen und Detailplanungen – über die gesamte IT-Umgebung hinweg. Gegner behaupten, dass solche Systeme nicht einsetzbar seien, weil sie zu große Probleme und Veränderungen im Arbeitsablauf bewirkten. Die Erfahrung gibt ihnen scheinbar recht: Obwohl die Technologie und die Produkte schon seit mehreren Jahren verfügbar sind, haben nur sehr wenige und sehr große Unternehmen, Banken oder öffentliche Einrichtungen bisher eine PKI aufgebaut.

Doch die PKI ist kein Alles-oder-Nichts-Projekt – sie kann auch in kleinen Schritten begonnen werden. Auf der Basis einer soliden Grundplanung kann eine Politik der kleinen Schritte langfristig schnell zum Erfolg führen. Wer nach und nach seine Verschlüsselungslösungen zusammenführt, kommt langsam zu einer PKI, die dadurch immer mehr an Bedeutung gewinnt. Unternehmen können sich so Zug um Zug mit PKI-Komponenten wie Smartcard, CA oder RA vertraut machen und nach und nach zu einer einheitlichen Authentisierung gelangen.

Denn dass PKI wichtig ist, daran zweifelt niemand. Letztlich kommt um PKI kein Unternehmen herum, das seine Netze Geschäftspartnern öffnet oder Mitarbeitern remote Zugriff gewährt. Ein Sammelsurium an Verschlüsselungsanwendungen, wie sie derzeit Usus sind, ist keine Lösung. Mit PKI besteht die Möglichkeit, diese Vielfalt auf einen gemeinsamen Nenner zu bringen – im Sinne einer höheren Sicherheit für das Unternehmen.

### 1.3.17 Teil II: PKI Fallstudien und Produkte

Der zweite Teil des Überblicks über Public-Key-Infrastrukturen widmet sich den praktischen Aspekten. Anhand kleiner Fallstudien wird gezeigt, wie Unternehmen ihre PKI aufbauen und welche Produkte und Dienstleister in diesem Segment eine Rolle spielen. Ein Wegweiser für weiterführende Informationsquellen nennt Anlaufstellen für Beratung und die wichtigsten PKI-Institutionen.

Entscheidende Voraussetzung für den Aufbau von PKIs ist die Verfügbarkeit von Software, die auf asymmetrischen Verfahren beruhende Sicherheitsdienste einsetzt. Dazu gehören neben Lösungen für die Installierung der PKI selbst auch die PKI-fähigen Anwendungen, die Applikationen wie sichere E-Mail-Kommunikation oder Verschlüsselung ermöglichen.

### 1.3.18 Utimaco Safeware

Als Basisapplikation zur Generierung, Überprüfung und dem Management von Zertifikaten offeriert Utimaco Safeware seine SafeGuard PKI. Das Produkt beruht auf offenen, internationalen Standards: Die Zertifizierungs- und Registrierungsinstanzen können über standardisierte Protokolle und Formate auf die Verzeichnissysteme anderer Anbieter zugreifen.

Die Standardversion SafeGuard PKI Enterprise stellt alle PKI-Funktionalitäten zur Ausstellung, Verteilung und zum Management von X.509-Zertifikaten einschließlich der Verwaltung von Sperrlisten zur Verfügung. Daneben ist eine Light-Version verfügbar, mit der sich PKI-Lösungen in sehr kurzer Zeit ohne viel Aufwand realisieren lassen: Das „Out-of-the-box“-Produkt SafeGuard PKI Light besteht aus den Komponenten CA und RA. Es lässt sich auch ohne Spezialisten einrichten und bietet alle Funktionen, die in kleineren und mittleren Unternehmen für das Generieren und Managen von Schlüsseln und Zertifikaten notwendig sind.

SafeGuard PKI dient als Infrastruktur und Basistechnologie für weitere PKI-Produkte von Utimaco:

- SafeGuard Sign & Crypt zur Integration von Verschlüsselung und digitaler Signatur in bestehende Anwendungen
- SafeGuard Transaction Client, ein Browser-Modul, um digitale Signaturen bei Internet-Transaktionen zu ermöglichen, und
- SafeGuard Toolkit, um Sicherheitsfunktionen in bestehende Anwendungen zu integrieren.

Außerdem unterstützt SafeGuard PKI in Verbindung mit SafeGuard Advanced Security und SafeGuard LAN Crypt auch die Verwendung von Smartcards. Preise werden auf Anfrage genannt.

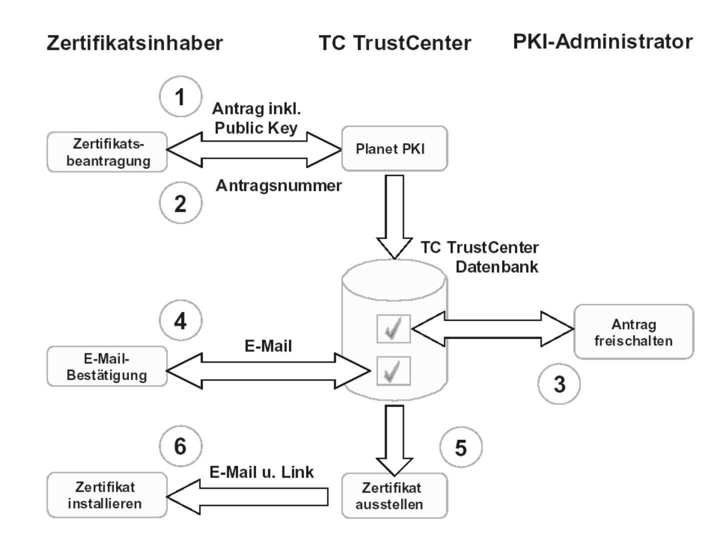
## 1.3.19 TC TrustCenter

Die Hamburger TC TrustCenter AG ist gemäß dem deutschen Signaturgesetz von der RegTP als Zertifizierungs-Diensteanbieter akkreditiert. Der Fokus des Unternehmens liegt auf der Beratung von Unternehmen, die maßgeschneiderte IT-Sicherheitsinfrastruktur-Lösungen aus einer Hand erwarten.

Mit TC PKI bietet TC TrustCenter ein modulares System für den Aufbau einer lokalen Public-Key-Infrastruktur zur Zertifikatsverwaltung an. Die Software dazu wird jedoch nicht lokal installiert: Sie liegt auf den Servern von TC TrustCenter und lässt sich über SSL-Verbindungen nutzen. TC PKI gibt es in zwei Varianten:

Die webbasierte PKI-Einstiegslösung für digitale Zertifikate heißt TC Entry PKI (249 Euro Monatsgebühr, Einrichtung 2250 Euro). Sie ermöglicht, User-ID und Passwort durch eine Client-Authentifikation per Zertifikat zu ersetzen. Zertifikate für 25 User und den Administrator auf Smartcard sowie ein Lesegerät und Software sind enthalten, weitere Zertifikate lassen sich online beantragen.

Als PKI-Standard-Lösung für Unternehmen fungiert TC PKI (Preis auf Anfrage). Damit ist die SSL-Verbindung der Clients zum Server ebenso möglich wie das Verschlüsseln von E-Mails. Die Zertifikate stellt der Administrator über eine Weboberfläche aus. Da TC TrustCenter die PKI-Software hostet, lassen sich alle Vorteile einer eigenen CA nutzen, ohne selbst eine aufwendige Implementation vornehmen zu müssen.




**TC TrustCenter:** TC Entry PKI ist eine webbasierte PKI-Lösung. Alle Komponenten einer PKI werden von TC Trustcenter über das Web zur Verfügung gestellt.

## 1.3.20 Secude

Das Portfolio der Secude GmbH reicht von Produkten zum Aufbau und Verwalten einer PKI über die Absicherung elektronischer Geschäftsprozesse bis hin zu PKI-gestütztem Single Sign-On für alle angebotenen Lösungen.

Als Basis zur Implementierung einer PKI dient Secude CA Management. Es ermöglicht den Aufbau und Betrieb einer vollständigen Zertifizierungs-Infrastruktur und stellt alle dazu notwendigen Dienste bereit. So kann man Zertifikate ausstellen und widerrufen, Sperrlisten pflegen, Benutzer verwalten sowie ein Logbuch führen. Secude CA Management beherrscht verschiedene Schlüsselgenerierungs- und Zertifizierungsmodelle. Die Benutzer können entweder ihre Schlüssel selbst erzeugen – in diesem Fall werden sie von der Zertifizierungsstelle nur bestätigt. Die CA kann aber die Schlüssel für die Benutzer auch direkt generieren. Optional lässt sich Secude CA Management zur Online-Zertifizierung direkt an einen Webserver anbinden.

iT_SEC_sci dient dazu, eine Smartcard-gestützte PKI aufzubauen. Um die Verwaltung möglichst komfortabel zu machen, verfügt iT_SEC_sci über umfangreiche Helpdesk-Funktionen. So können etwa durch fehlerhafte PIN-Eingaben gesperrte Karten in wenigen Minuten entsperrt werden. Dazu muss der Benutzer nur beim Helpdesk anrufen. Außerdem beinhaltet iT_SEC_sci ein Karten-Management mit integrierter Benutzer-, Smartcard- und Schlüsselverwaltung.

SECUDE AuthenteMail bietet E-Mail-Sicherheit für Outlook und Lotus Notes. Es ermöglicht den Benutzern den vertraulichen Austausch von Mails. Dabei stellt es mit Hilfe einer digitalen Signatur sicher, dass der Inhalt der E-Mail nicht verändert wurde. Eine digitale Signatur lässt zudem den Urheber eindeutig erkennen. Als Speicher für die notwendigen Schlüssel können sowohl Software- als auch Hardware-Token (Smartcard, USB-Token, etc.) eingesetzt werden.

Als Encryption-Mechanismen setzt AuthenteMail international als sicher anerkannte Algorithmen wie RSA, DAS, Triple DES oder SHA1 ein. Neben der Sicherheit ist auch die Interoperabilität von großer Bedeutung. Daher unterstützt das als Plug-in ausgelieferte SECUDE AuthenteMail for Outlook die Standards S/MIME und MTT.

Preise nennt Secude nur auf konkrete Anfrage, da sie von der jeweiligen Lösung sowie der Anzahl der Zertifikate abhängen.

## 1.3.21 Integralis

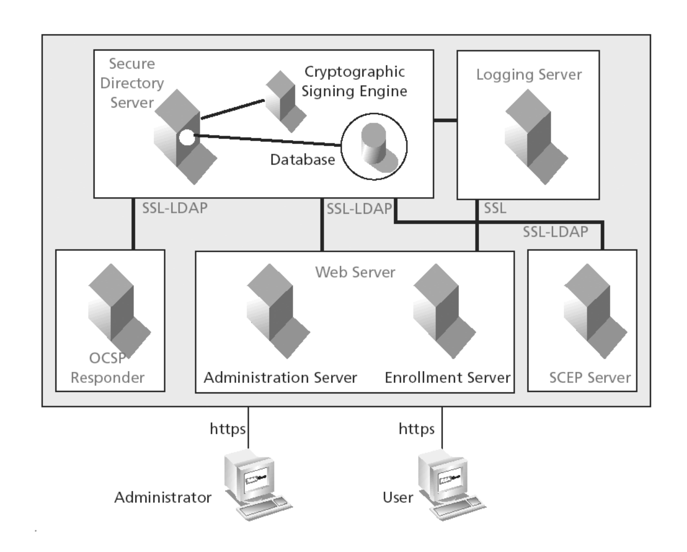
Integralis operiert als produktunabhängiger Integrator für IT-Sicherheitslösungen. Dabei betrachtet man PKI in der Regel nur als eine von mehreren Möglichkeiten, entsprechende Sicherheitsbedürfnisse abzudecken. Zu den Alternativen respektive Ergänzungen zählt Integralis Einmal-Passwort-Token oder auch Single Sign-On bzw. Reduced Sign-On über normale Benutzername/Passwort-Verfahren.

Bei Integralis PKeasy handelt es sich um ein Produkt zur einheitlichen Verschlüsselung und Authentisierung in Unternehmen. Die Basis der Lösung bilden ausgewählte Anwendungen für Dateiverschlüsselung, VPN / Remote Access und Mailverschlüsselung. Eine Smartcard oder ein USB-Token dient dabei als Firmenausweis, Schlüssel, zentraler Lagerort für Benutzerdaten sowie Speicher für mehrere Passwörter und PIN-Codes.

## 1.3.22 RSA Security

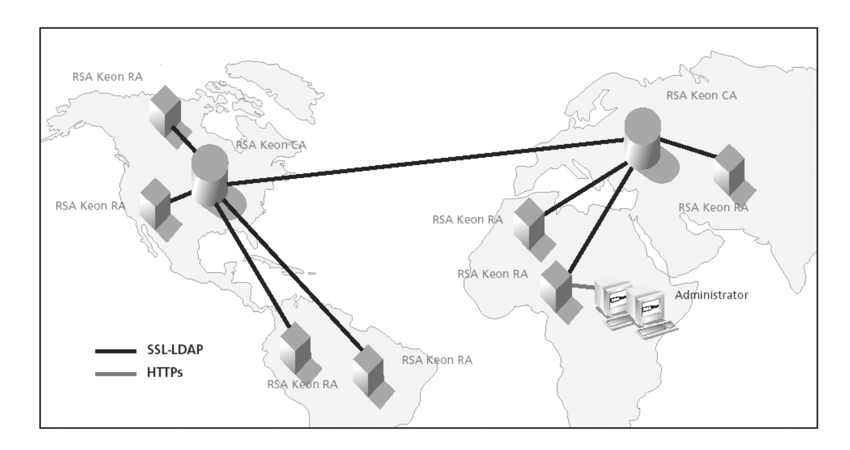
Mit Keon von der US-Firma RSA Security lassen sich unternehmensinterne PK-Infrastrukturen aufbauen, managen und nutzen. Mit der Software können digitale Zertifikate erstellt und verwendet und digitale Signaturen für rechtsverbindliche Transaktionen eingesetzt werden. RSA Keon bietet insbesondere folgende Features:

- Nichtabstreitbarkeit elektronischer Verträge durch digitale Signaturen.
- Sicherung von strategisch wichtigen Webportalen.
- Positive Identifikation eines Absenders oder Vertragspartners.
- Überprüfung der Integrität und des privaten Charakters von Daten in E-Commerce-Anwendungen.
- Verschlüsselung von sensiblen Daten und vertraulicher Kommunikation, deren Inhalt nur der Empfänger sehen kann.




**RSA Security:** Die Architektur von Keon CA im Überblick. (Quelle: RSA Security)

Das automatische Management von öffentlichen und privaten Schlüsseln gewährleistet eine einfache Nutzung. Keon ist als zentrale Zertifizierungsstelle (RSA Keon CA) oder als komplette PKI-Lösung verfügbar. Als weitere Produkte offeriert der Hersteller RSA BSAFE, eine Verschlüsselungs-Software zur Sicherstellung der Datenintegrität und RSA SecurID zur Autorisierung von Datenzugriffen. Preise gibt es auf Anfrage von der deutschen Niederlassung.




**RSA Security:** Mit RSA Keon RA lassen sich verteilte PKIs realisieren.

## 1.3.23 D-Trust

Die Berliner D-TRUST bietet Unternehmen, Verbänden und Behörden ein breites, an Standards orientiertes Portfolio rund um die digitale Signatur. Die Produkte sind vorkonfiguriert, lassen sich aber auch individuell anpassen. Im Zentrum steht die Trust-Center-Lösung D-TRUST Corporate, mit der sich CAs für Personen, VPN-Rechner und Webserver realisieren lassen.

Die modulare Unternehmens-PKI auf Software-Basis wurde von der skandinavischen Firma SmartTrust (früher: ID2) entwickelt. Registrierung und Karten-Personalisierung werden exakt an die organisatorischen Bedürfnisse und betrieblichen Möglichkeiten des Unternehmens angepasst. Dabei kommen je nach Bedarf verschiedene Modelle zum Einsatz.

Bei D-TRUST Corporate CRA befindet sich der Registrierungsarbeitsplatz im Unternehmen. Zertifikate und Smartcards werden dann im D-TRUST Center erstellt. Dieses Modell ist in besonderem Maße auf das Ausgeben von Zertifikaten an Mitglieder und Geschäftspartner zugeschnitten. D-TRUST Corporate CRP übernimmt über die Registrierung hinaus auch die unternehmensinterne Personalisierung der Smartcards.

Dieses Modell eignet sich besonders für die paralelle Nutzung der Smartcards als Dienst- bzw. Mitarbeiterausweise. D-TRUST Corporate DSC belässt sämtliche Registrierungs- und Personalisierungsprozesse bei D-TRUST. Dieses Modell bietet sich an, wenn hohe Sicherheitsanforderungen einen Einsatz von Inhouse-Komponenten verbieten.

Mit D-TRUST P-Zert lassen sich nicht nur Zertifikate verwalten, sondern auch gesetzeskonforme digitale Signaturen generieren. Das Produkt wird in vier Varianten angeboten:

- D-TRUST P-Zert Q entspricht voll den signaturgesetzlichen Vorgaben („qualifiziertes Zertifikat").
- D-TRUST P-Zert A entspricht darüber hinaus den strengeren Vorgaben für akkreditierte Zertifikate.
- D-TRUST P-Zert F als „fortgeschrittenes Zertifikat" bietet sichere Smartcard-Technik ohne die signaturgesetzlichen Beschränkungen.
- D-TRUST P-Zert S, ebenfalls „fortgeschrittenes Zertifikat" im Sinne des Signaturgesetzes, arbeitet Software-basiert.

Außerdem bietet D-Trust PKI-Hardware und -Software für den Aus- und Eigenbau von PK-Infrastrukturen an. D-Trust übernimmt daneben auch die Beratung und das Projektmanagement.

## 1.3.24 T-TeleSec

T-TeleSec, das Trustcenter der Deutschen Telekom, hat verschiedene Produkte und Services für eine Unternehmens-PKI im Programm. Dazu zählen die Trust Center Services wie ServerPass, OneTimePass, MailPass und NetPass (letztere zur Zeit noch im Projektgeschäft, ein Vertriebsfreigabe steht aber bevor). Der ServerPass dient zur Identifikation eines Internet-Servers. Der OnlinePassTest ist das Gegenstück zum ServerPass. So wie sich ein Unternehmen durch einen ServerPass identifiziert, weist man sich mit dem OnlinePass gegenüber dem Unternehmen aus.

Dazu kommen Smartcards, die mit Zertifikaten für Verschlüsselung und elektronische Signatur genutzt werden können. Als SigG-konformen Service für qualifizierte Signaturen hat T-TeleSec zudem den Public Key Service im Portfolio, der im Sinne des Signaturgesetzes (SigG) offiziell zugelassen ist. Damit lassen sich Verträge oder vertrauliche Daten digital unterzeichnet werden, Bezahl- und Bestellvorgänge im E-Commerce sichern sowie Datensätze vor Manipulationen schützen.

Das Programm PKSCrypt schließlich dient zum Signieren und Verifizieren von Daten, zur Verwaltung der entsprechenden PKS-Zertifikate, zur Nutzung des signaturgesetzkonformen Zeitstempeldienstes und zum Verschlüsseln und Entschlüsseln von Daten. Die Software erweitert die Funktionalität des Windows-Explorer.

## 1.3.25 Baltimore Technologies

Der PKI-Anbieter Baltimore liefert mit seiner Trusted Business Suite eine PKI in Light-Version. Der US-Security-Spezialist mit europäischer Niederlassung beschränkt sich dabei auf den kleinsten gemeinsamen Nenner: Die Suite stellt nur das zur Verfügung, was alle brauchen.

Die Installationszeit beschränkt sich dadurch auf maximal drei Tage. Baltimore berücksichtigt damit die Bedenken vieler Anwender, die der PKI-Technologie vorwerfen, sie wäre zu schwierig, langwierig und kostspielig zu implementieren.

Ausgeliefert wird eine komplette PKI mit limitierenden Regeln. Das geht zwar auf Kosten der Flexibilität, deckt aber die meisten Normalfälle ab. Zusätzlich zur PK-Infrastruktur stellt Baltimore die kompletten Anwendungen zur Verfügung. Als Basiskomponente dient die Applied Solution Engine, die auf dem Unternehmensserver installiert wird und die das limitierte Regelwerk der Policy beinhaltet.

Die Beschränkungen können beispielsweise darin bestehen, dass das Document Handling nur mit PDF- und DOC-Dateien erfolgt, nicht hingegen mit Wordperfect-Files. Ebenfalls in der Suite enthalten sind die Module Document Signing, Form Signing, E-Mail, VPN, Web Access und Networks. Preis: ab 60.000 Euro.

## 1.3.26 Microsoft

Eine „PKI light“ kann man auch mit Windows 2000 realisieren. Die Server-Variante des Betriebssystems bietet im Standardlieferumfang bereits PKI-Komponenten an, die sich zum Aufbau einer unternehmensweiten PKI nutzen lassen.

Im Active Directory ist bereits eine PKI integriert. Sie empfängt und validiert Zertifikatsanfragen. Außerdem generiert, veröffentlicht und widerruft sie Zertifikate. Die dabei verwendeten CAs können sowohl von Windows 2000 selbst (etwa vom Encrypting File System EFS) als auch von externen Komponenten (Kunden, Geschäftspartner, Software von Drittherstellern) verwendet werden.

Im Rahmen des PKI-Konzeptes gilt es dabei eine ganze Reihe von Aspekten zu regeln. Dazu zählen die hierarchische Struktur von CAs, deren Vertrauensstellungen zueinander, sowie den Einsatzzweck und die Verteilung von Zertifikaten an Benutzer und innerhalb des Systems.

Die neue Windows-Server-PKI wurde im Vergleich zum Vorgänger weiter verbessert. So können jetzt Computer- und Nutzerzertifikate automatisch ausgeliefert werden, was den Weg zum Helpdesk erspart. Außerdem überarbeitete Microsoft auch die Generierung und Archivierung der Schlüssel.

## 1.3.27 Fallstudien für PKI-Lösungen

Hauptanwender von PK-Strukturen sind derzeit vor allem Behörden, Institutionen und Großkonzerne. Mittelständische Unternehmen scheuen das Thema wegen der hohen Komplexität von PKI noch weitgehend. Die wenigen Unternehmen, die bereits eine PKI installiert haben, wollen oft aus verständlichen Gründen mit ihren Lösungsansätzen nicht an die Öffentlichkeit gehen. Ist eine Firma doch bereit, ihre PK-Struktur offen zu legen, spart sie die interessanten Details meist aus.

Trotz dieser Schwierigkeiten konnten wir einige interessante Studien aus unterschiedlichen Gebieten zusammenstellen. Anhand dieser Beispiele lässt sich zumindest im Ansatz erkennen, wie Unternehmen ihre PKI umsetzen, welche Zwecke sie damit verfolgen, auf welche Produkte und Lösungen sie setzen und schließlich: Was ihnen die PKI konkret bringt.

## 1.3.28 Sicherer Strom, sichere Reifen

Ende 2002 entschied sich der international operierende Kraftwerkskonzern Steag (www.steag.de) aus Essen für die TC TrustCenter AG als „Lieferant von Sicherheit" für das Unternehmensnetzwerk und die Unternehmenskommunikation.

Im dem Projekt wurde in der ersten Phase ein Drittel der über 3.300 Mitarbeiter der Steag AG mit digitalen Zertifikaten von TC TrustCenter zur Absicherung der in- und externen Kommunikation ausgestattet. Die Mitarbeiter des Konzerns versenden täglich sicherheitskritische Daten über das Internet. In der zweiten Ausbaustufe sollen Smartcard-basierte Zertifikate ausgegeben werden. Neben den bisherigen Funktionen wie Zeiterfassung oder Zugangskontrolle lassen sich dann zusätzliche Einsatzgebiete wie Virtual Private Network (VPN) erschließen.

In späteren Phasen sollen unterschiedliche Anwendungen an die Sicherheitsinfrastruktur angebunden werden: Systemanmeldung (Single Sign-On) und die Einbindung komplexer Applikationen wie Enterprise Resource Planning-Systeme (ERP-Systeme). Das soll Steag Investitionssicherheit garantieren; das Unternehmen kann eine Vielzahl von Anwendungen abbilden und um modulare Komponenten erweitern. Die Einsparpotenziale bei der Digitalisierung von Geschäftsprozessen schätzt man auf 20 und 40 Prozent.

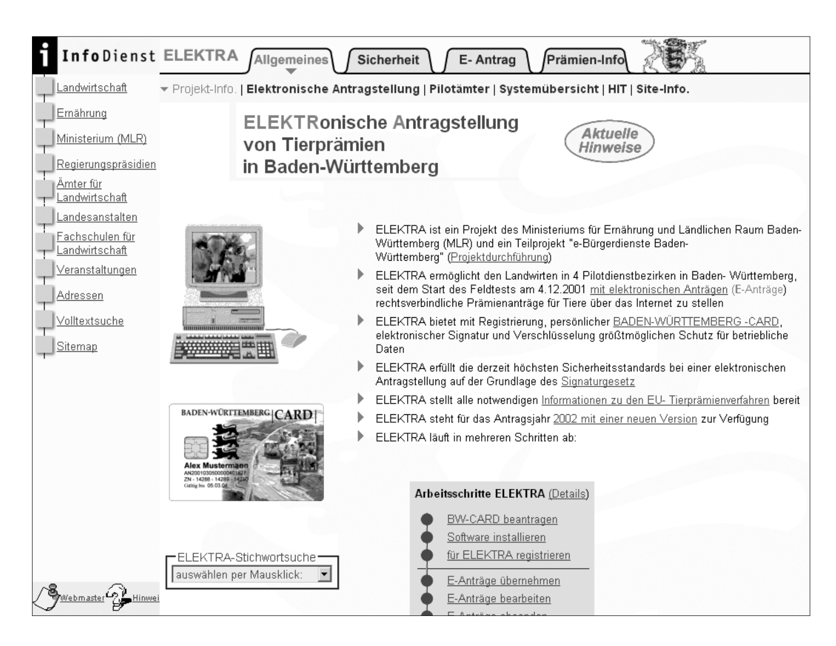
Ebenfalls auf TC Trustcenter setzt der Reifenhersteller Continental AG (www.conti-online.com). Mit dem Projekt ContiOnlineContact bietet das Unternehmen seit 1997 dem Reifenfachhandel ein Informations- und Transaktionssystem an, das neben vielseitigen Serviceangeboten Verfügbarkeitsanfragen und Online-Bestellungen ermöglicht.

Entwicklung und Betrieb dieses Systems gewährleistet die ICA GmbH, ein Gemeinschaftsunternehmen von Continental und IBM Deutschland. Seit Juli 1999 steht ContiOnlineContact dem europäischen Reifenhandel auch als Webservice im Internet zur Verfügung.

## 1.3.29 Elektronische Landwirtschaft

Die Anwendung ELEKTRA (Elektronische Antragstellung) ermöglicht es den Landwirten in Baden-Württemberg, Prämienanträge für Tiere über das Internet zu stellen. Dazu zählen Mutterkuhprämie, Schlachtprämie sowie Sonderprämie für Rinder. Durch die elektronische Datenerfassung ergeben sich Einsparungen für die Landwirtschaftsverwaltung sowie eine bessere Datenqualität. ELEKTRA (www.infodienst-mlr.bwl.de/elektra/start.htm) ist ein Gemeinschaftsprojekt der Datenzentrale Baden-Württemberg im Auftrag des zuständigen Ministeriums (MLR) und der Secude GmbH (www.secude.de).

Da es sich bei den Prämienanträgen um hochsensitive Daten handelt, mit denen Auszahlungen von Fördermitteln der Europäischen Union verbunden sind, wurde an die Sicherheitskonzeption für das Verfahren ELEKTRA höchste Ansprüche gestellt. Um den Antragsteller eindeutig zu identifizieren, müssen alle Landwirte, die am Verfahren teilnehmen wollen, eine Signaturkarte beantragen. Diese wird durch die Deutsche Post Signtrust (www.signtrust.de) mittels des PostIdent-Verfahrens identifiziert.




**Baden-Württemberg:** ELEKTRA lässt sich von jedem Interessenten online testen – auch ohne die erforderliche Sicherheitssoftware und ohne eine BW-CARD. Anhand von Daten aus Testbetrieben kann das System ausprobiert werden.

Erst nach Erhalt der Signaturkarte kann sich der Landwirt im Internet unter www.elektra.bwl.de zur Teilnahme am Verfahren anmelden. Nur wenn die Angaben auf seiner Karte und seine Unternehmens-ID mit den beim Ministerium gespeicherten Daten übereinstimmen, wird der Landwirt zum Verfahren zugelassen. Er kann dann Prämienanträge vom ELEKTRA-Server herunterladen.

Alle Daten werden signiert übertragen. Der Landwirt muss also jede Transaktion (sowohl die Anforderung als auch die Abgabe von Prämienanträgen) elektronisch unterschreiben. Auch der Server unterzeichnet jeglichen verwendeten Code mittels „Codesigning-Zertifikaten“, was eine eindeutige Zuordnung ermöglicht. Alle Daten, die vom Server an den Landwirt gehen (Prämienanträge, Fehlermeldungen, Quittungen, etc.) werden mittels eines IBM-Cryptoboards unterzeichnet.

Derzeit wird die Baden-Württemberg-Card (BW-Card) der Deutschen Post Signtrust zur elektronischen Signatur verwendet. Es besteht aber durchaus die Möglichkeit, auch andere Signaturkarten einzubinden, soweit sie den vorgegebenen Sicherheitsstandards entsprechen.

Innerhalb des Verfahrens basieren alle Transaktionen auf dem Protokoll HTTP 1.1 und werden mit einem 128-Bit-Key SSL-verschlüsselt. Zur Erhöhung der Ausfallsicherheit stehen im Rechenzentrum des MLR zwei Server zur Verfügung, die einen lückenlosen Betrieb der Anwendung garantieren sollen.

## 1.3.30 Personaldaten verschlüsselt übertragen

Die Siemens AG hat sich für die Einführung der Standard-Software SAP R/3 HR (Human Resources) entschieden. Sie dient zur Personaladministration und Abrechnung der 200.000 Siemens-Mitarbeitern sowie der 135.000 Pensionäre. Die zentrale Anforderung bei der Einführung von SAP R/3 HR war der Aufbau einer Sicherheitsinfrastruktur, die den Anforderungen des Datenschutzes und der Informationssicherheit gerecht wird.

Als größte Schwachstelle des Systems sah man die ungesicherte Kommunikation auf der Netzwerkebene an. Über diese Schwachstelle hätten potenzielle Angreifer Anmeldeinformationen und Passwörter ausspähen oder Daten mitlesen, manipulieren und weiterleiten können. Demgemäß kam kam nur die Verwendung eines Produkts zur Software-Verschlüsselung in Frage. Die Wahl fiel dabei auf Secude für R/3, ein von SAP zertifiziertes Produkt von Secude, das über eine Schnittstelle an SAP angebunden ist.

Die sichere Verbindung zwischen den SAP-Clients und den Applikationsservern wird über Secude aufgebaut. Bei der Anmeldung eines Clients an das SAP-System läuft im Hintergrund die so genannte Drei-Wege-Authentisierung an. Dabei authentisiert sich sowohl der Client dem Applikationsserver gegenüber als auch umgekehrt der Server gegenüber dem Anwender. Die Grundlage dafür bildet das so genannte PSE (Personal Security Environment), das die Gesamtheit des Schlüsselmaterials umfasst.

Bei der Benutzerauthentifikation mit Secude gegenüber einem R/3-Server erfolgt ein Austausch der digitalen Signatur. Dabei gibt der Nutzer einmalig vor Beginn der R/3-Sitzung die PIN ein, mit der er sich lokal gegenüber seinem PSE auf dem Firmenausweis authentisiert. Während der Drei-Wege-Authentisierung wird auf beiden Seiten eine Vertrauensbasis als Grundlage der Verschlüsselung etabliert.

Die generierten Schlüssel gelten exklusiv für eine Session und sind nur den beiden Partnern bekannt. Meldet sich der Anwender vom R/3-System ab, verwirft dieses die Schlüssel. Einer Schlüssellänge von 1024 Bit und die im Anschluss daran aktivierten Verschlüsselung der Datenübertragung mit 168 Bit bieten ein Höchstmass an Kommunikationssicherheit.

## 1.3.31 Justizbehörde: Biometrische Authentifikation

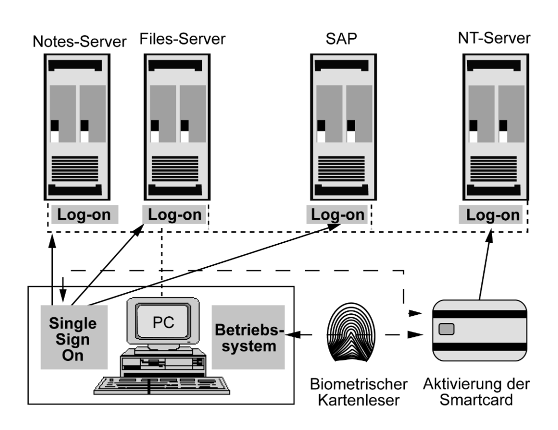
Im Rahmen des Projekts ROBIN wird zum weltweit ersten Mal biometrische Technik großflächig zur Absicherung von IT-Systemen in der öffentlichen Verwaltung eingesetzt. Kern des Projekts, das im November 2001 vom niederländischen Justizministerium in Auftrag gegeben wurde, ist die Bereitstellung einer sicheren IT-Umgebung für die „Richterlichen Organisationen" der Niederlande. Die PKI wurde mit Utimaco-Technologie umgesetzt.

Bislang herkömmlich abgewickelte Verwaltungsprozesse sollen künftig auf elektronischem Weg durchgeführt werden, ohne an Sicherheit einzubüßen. Um die Verbindlichkeit und Vertraulichkeit sämtlicher Vorgänge zu gewährleisten, bindet man Identifikation und Authentisierung, Ver- und Entschlüsselung sowie die digitale Signatur mit Hilfe biometrischer Verfahren an den einzelnen Nutzer.

Um ein dem Verwendungszweck angemessenes Sicherheitsniveau zu erreichen, kombiniert das Verfahren mehrerer Mechanismen. Dazu zählen:

- starke Authentifikation mit biometrischen Verfahren,
- Dateiverschlüsselung,
- E-Mail-Sicherheit durch Verschlüsselung und digitale Signatur,
- PKI, sowie
- die eindeutige Koppelung der digitalen Identität (des Zertifikats) an die natürliche Person. Dazu dienen personengebundene Smartcards mit Fingerabdruckvergleich.

Als zentrales Sicherheits-Token kommt die persönliche Smartcard zum Einsatz. Sie speichert das Zertifikat des jeweiligen Nutzers, seine Passworte für sämtliche Netz-Ressourcen sowie seine Private Keys. Damit lässt sie sich zur Authentisierung an PCs, Servern und Host-Systemen, zur Verschlüsselung von Dateien und E-Mails sowie für digitale Signaturen verwenden. Die Sicherheitsinfrastruktur basiert auf einer PKI, welche die Registrierung der Nutzer, die Schlüsselerzeugung, die Ausgabe von Zertifikaten und Smartcards sowie die Bereitstellung von Verzeichnisdiensten und Sperrlisten organisiert.



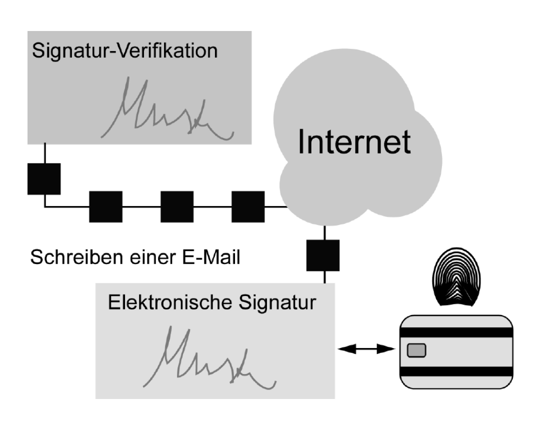

**Biometrische Authentifikation:** Zur Anmeldung im Netzwerk wird der Benutzer über einen Fingerabdruck identifiziert.



Möchte der Benutzer auf seinen Arbeitsplatzrechner zugreifen, dann fordert die Sicherheitssoftware ihn auf, seine Smartcard einzulegen und mit Hilfe seines Fingerabdrucks frei zu schalten. Nach erfolgreicher Aktivierung der Smartcard wird damit ein „Advanced Security Log-On“ durchgeführt. Anschließend kann der Benutzer die ihm erlaubten Aktionen auf dem PC durchführen.

Auch beim Aufruf authentisierungspflichtiger Dienste auf einem Server wird zwischen der Security Software auf dem Server und der Smartcard eine kryptographische Authentisierung durchgeführt.

Zur Erzeugung der elektronischen Signatur unter einer E-Mail legt der Nutzer seine Smartcard ein und authentisiert sich per Fingerabdruck. Hat er sich bereits mit Smartcard und Fingerabdruck eingeloggt hat, kann er die gleiche Smartcard für die digitale Signatur und Verschlüsselung von E-Mails nutzen. Die dafür benötigten Schlüssel sind ebenfalls auf der Karte gespeichert.

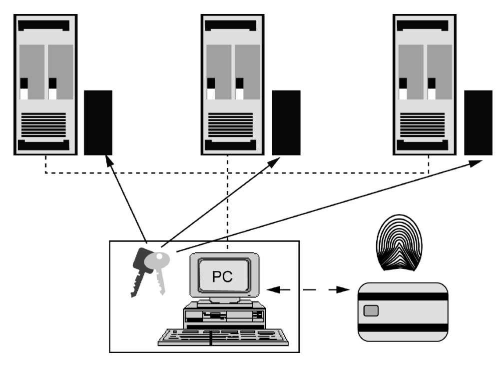



**Biometrische Authentifikation:** Aktivierung der elektronischen Signatur.

Dateiverschlüsselung sorgt dafür, dass Mitarbeiter Dokumente über das Unternehmensnetz austauschen und im Netzwerk ablegen können, ohne dass diese von Unbefugten gelesen oder bearbeitet werden könnten. Die Benutzergruppen richtet der Administrator so ein, dass nur bestimmte User eine Zugangsberechtigung und damit einen Schlüssel für die sensiblen Dokumente besitzen.

Auch hier ist die Authentisierung mit Smartcard und Fingerabdruck der sicherste und einfachste Weg für die Benutzer. Um Zugriff auf die Daten zu bekommen, wird das Dateiverschlüsselungssystem auf dem PC durch den Fingerabdruck aktiviert. Dieses System verwendet den auf der Smartcard gespeicherten Schlüssel, um die Daten zu entschlüsseln.

Für die befugten Nutzer läuft dieser Vorgang transparent, also ohne ihr Zutun ab. Für alle anderen bleiben die Daten mangels Schlüssel unlesbar. Die Daten werden in verschlüsselter Form vom Fileserver über das Netzwerk auf den Computer des Anwenders übertragen und erst dort entschlüsselt.




**Biometrische Authentifikation:** Aktivierung der File-Verschlüsselung.

© tecChannel.de

Das Projekt ROBIN verdeutlicht, dass Benutzerkomfort und Bequemlichkeit in Verbindung mit Sicherheitsfunktionen wichtige Erfolgsfaktoren für die Verwendung von Sicherheitsmechanismen sind. Biometriefähige Sicherheitsanwendungen und Smartcards sowie eine PKI-basierte Sicherheitsinfrastruktur bilden die Grundlage eines entsprechenden Konzepts.

## 1.3.32 PKI in der Stadtverwaltung

Wie führt man konkret eine PKI-Struktur ein? Die Stadt Karlsruhe verfolgt das Ziel eine gesicherte elektronische Kommunikation für stadtinterne Zwecke zu schaffen. Sie stellt im Web ein umfangreicheres Dokument zur Verfügung, das die Arbeitsrichtlinien ihrer Zertifizierungsstelle beschreibt. Das Papier lässt sich durchaus auch auf eigene Zwecke übertragen. Man findet es unter der Adresse http://193.197.165.50/Stadt/Ver/CA/arb_richtl.htm.

## 1.3.33 Anlaufstellen für PKI und weiterführende Informationsquellen

Die folgende Tabelle listet die wichtigsten PKI-Anlaufstellen und weiterführende Informationsquellen im Internet auf.

| **Weiterführende PKI-Quellen** | | |
|---|---|---|
| **Institution** | **Information** | **URL** |
| **Behörden** | | |
| Bundesamt für Sicherheit in der Informationstechnologie (BSI) | Umfassende Infos mit Projekten, Fachbeiträgen, Veranstaltungen | www.bsi.de |
| Regulierungsbehörde für Telekommunikation und Post (RegTP) | Informiert über deutschen TK Markt | www.regtp.de |
| Verzeichnisdienst der RegTP | Verzeichnisdienst der Regulierungsbehörde für Telekommunikation und Post. Hier können Zertifikate online geprüft werden. | www.nrca-ds.de |
| Projektbüro „Digitale Signatur“ des Bundesamts für Sicherheit in der Informationstechnik (BSI) | Beratung und Unterstützung über die elektronische Hotline | www.bsi.bund.de/esig |
| **Recht** | | |
| Signaturgesetz | Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften | www.signaturrecht.de |
| Bundesamt für Wirtschaft und Arbeit | Informations- und Kommunikationsdienstegesetze | www.iid.de/iukdg/index_esig.html |

| **PKI-Institutionen, -Vereine** | | |
|---|---|---|
| PKI-Forum | Zusammenschluss von Unternehmen, um PKI technisch und wirtschaftlich voranzubringen | www.pkiforum.org |
| Teletrust Deutschland | Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik | www.teletrust.de |
| PKI Page | PKI-Infos und alle Links auf CAs in den wichtigste Ländern | www.pki-page.org |
| Security-Server Uni Siegen | Technische Aspekte der PKI | www.iid.de/iukdg/index_esig.html |
| Sicherheit im Internet | Ausführliche Security-Infos des Innen- und Wirtschaftsministeriums | www.sicherheit-im-internet.de |
| **Zertifizierungsstellen** | | |
| Telesec | Trustcenter der Deutschen Telekom | www.telesec.de |
| TC Trustcenter | Trustcenter Bundesverband Deutscher Banken | www.trustcenter.de |
| Signtrust | Trustcenter Deutsche Post (z.Z. nur eingeschränkt) | www.signtrust.de |
| De-Coda | 100%ige Tochtergesellschaft des Deutschen Industrie- und Handelstages in Bonn | www.de-coda.de |
| Deutsches Forschungsnetz | Die Policy Certification Authority (PCA) ist die Zertifizierungsinstanz für das Deutsche Forschungsnetz. Hier werden unterschiedliche Zertifikate angeboten. | www.cert.dfn.de |

| Interoperabilität | | |
|---|---|---|
| ISIS | Vereinheitlichte ISIS-MTT-Spezifikationen für Interoperabilität und Testsysteme | www.t7-isis.de |
| European Bridge CA | Gegenseitige Anerkennung von Zertifikaten im Firmen- und Bankenbereich | www.bridge-ca.org |

## 1.3.34 Fazit

Der Markt bietet inzwischen eine breite Palette an PKI-Software und -Lösungen für jeden Bedarf. Es gilt, in der Fülle des Angebots auf das richtige Produkt und den richtigen Dienstleister zu setzen. Beratung ist hier unumgänglich.

Angesichts der Komplexität der PKI-Applikationen gehen derzeit einige Lösungsanbieter wie Utimaco oder Baltimore dazu über, abgespeckte PKI-Produkte auf den Markt zu bringen. Diese Light-Versionen gehen zwar mit funktionalem Verzicht und eingeschränkter Flexibilität einher. Sie bieten aber eine attraktive Alternative für kleinere und mittlere Unternehmen, die einen „weichen" PKI-Einstieg bevorzugen. Die Light-PKIs sind einfach handhabbar und kostengünstig, Consulting-Gebühren können entfallen oder zumindest minimiert werden.

Bislang existieren noch kaum Erfahrungsberichte für diese Produkte. Die vorliegenden, auf mittlere bis große Lösungen setzenden Fallstudien zeigen aber, dass sich mit der richtigen PKI-Anwendung die Sicherheit im Unternehmen entscheidend verbessern kann. Zudem können PKIs ein Berächtliches Einsparungspotenzial bieten.

Klaus Manhart

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Security im Überblick | a1068 | – |
| Kryptographie-Grundlagen | a416 | – |
| Praxis der digitalen Signatur | a909 | – |
| Elektronisch unterschreiben | a402 | – |

## 1.4 Firewall-Grundlagen

Die Sicherheit steht an erster Stelle, wenn das private Netzwerk eines Unternehmens (LAN) mit dem Internet verbunden ist. Eine zunehmende Anzahl von Mitarbeitern braucht Zugang zu Internet-Diensten wie dem WWW, E-Mail, FTP und Remote-Verbindungen (Telnet, SSH). Unternehmen wollen zudem für ihre Webseiten und FTP-Server den öffentlichen Zugang über das Internet ermöglichen.

Dabei muss die Sicherheit der privaten Netze gegenüber unautorisierten Zugriffen von außen gewährleistet sein. Der Administrator muss das lokale Netzwerk gegen das große Chaos „Internet“ abschirmen, damit Daten nicht in unbefugte Hände geraten oder gar verändert werden. Für Firmen, die vom Internet-Zugang abhängig sind, stellen auch die so genannten DoS-Attacken eine große Gefahr dar.

Mit Firewalls lassen sich Netzwerke gegen unbefugte Zugriffe von außen absichern. Die verfügbaren Lösungen reichen von der Zusatz-Software bis zu speziellen Geräten, die ausschließlich auf diese Aufgabe ausgelegt sind. In ihrer grundlegenden Funktionsweise unterscheiden sich die Systeme allerdings nur wenig.

### 1.4.1 Definition einer Firewall

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hardware und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz, wie zum Beispiel dem Internet.

An dieser „Brandschutzmauer“ entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind. Damit eine Firewall effektiv arbeiten kann, muss entsprechend der gesamte Datenverkehr zwischen dem privaten Netz und dem Internet über diese Station laufen. Die Firewall untersucht alle Pakete und lässt nur die unverdächtigen passieren.

Dabei muss die Firewall ihrerseits immun gegen Eindringlinge sein. Was würde eine Firewall nutzen, wenn Hacker sie nach Belieben anpassen könnten? Daraus lässt sich eine „Schwäche“ von Firewalls ableiten: Diese Systeme bieten keinen Schutz, sobald es einem Angreifer gelungen ist, sie zu überwinden. Daher ist auf die eigene Sicherheit der Firewall ebenso viel Augenmerk zu richten wie auf die Sicherheit des privaten Netzes selbst, die durch die Firewall gewährleistet werden soll.

Eine Firewall ist nicht wie ein Router, ein Bastion-Host oder ein anderes Gerät ein Teil des Netzwerks. Sie ist lediglich eine logische Komponente, die ein privates Netz vor einem öffentlichen Netz schützen soll. Ohne eine Firewall wäre jeder Host im privaten Netz den Attacken von außen schutzlos ausgeliefert. Das bedeutet: Die Sicherheit in einem privaten Netz wäre von der Unverwundbarkeit der einzelnen angeschlossenen Rechner abhängig und somit nur so gut wie das schwächste Glied im Netz.

### 1.4.2 Zentraler Sicherheitsknoten

Der Vorteil einer zentralen Firewall ist, dass sie das Sicherheitsmanagement vereinfacht. Damit gilt die von ihr hergestellte Sicherheit für das gesamte Netz und muss nicht für jeden Rechner einzeln definiert werden. Die Überwachung geschieht ebenfalls zentral über die Firewall. So kann sie gegebenenfalls auch einen Alarm auslösen, da Angriffe von außen nur über diese definierte Schnittstelle zwischen den Netzen erfolgen können. Das Erkennen eines Angriffs ist der erste Schritt zur Abwehr des Angreifers.

Als in den letzten Jahren die Internet-Adressen knapp wurden, trat auch in Unternehmen eine Verknappung von IP-Adressen (**webcode: a209**) ein. Eine Internet-Firewall ist in diesem Zusammenhang die geeignete Stelle zur Installation eines Network Address Translator (NAT), der die Adressenknappheit lindern kann. Und schließlich eignen sich Firewalls auch, um den gesamten Datenverkehr von und zum Internet zu überwachen. Hier kann ein Netzwerk-Administrator auch Schwachstellen und Flaschenhälse erkennen.

### 1.4.3 Nachteile und Begrenzungen

Eine Firewall kann keine Angriffe abwehren, wenn die Pakete nicht durch sie hindurch geleitet werden. Wenn zum Beispiel eine Einwählverbindung via Modem oder ISDN aus dem geschützten Netzwerk besteht, können interne Benutzer eine direkte PPP-Verbindung zum Internet aufbauen. Benutzer, welche die zusätzliche Authentifizierung am Proxy-Server scheuen, werden schnell diesen Weg nehmen. Durch die Umgehung der Firewall erzeugen sie jedoch ein großes Risiko für eine Backdoor-Attacke.

Auch bei Angriffen aus den eigenen Reihen nützt eine Firewall nichts. Sie hindert niemanden daran, sensitive Daten auf eine Diskette zu kopieren und sie außer Haus zu schaffen. Erst recht nicht, wenn diese Person weit reichende Rechte hat oder durch Diebstahl an Passwörter gelangt ist.

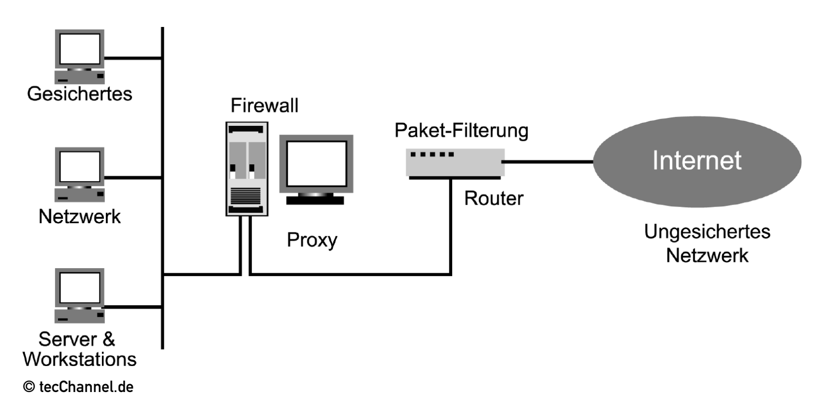
Firewalls bieten ebenfalls keinen Schutz vor Computerviren oder Trojanern, da sie nicht jedes Datenpaket nach potenziellen Schädlingen durchsuchen können. Daneben verhindern Firewalls auch keine so genannten Data-driven Attacks . Dabei handelt es sich um scheinbar harmlose Daten mit verstecktem Code zur Änderung von Sicherheitseinstellungen.

Zu guter Letzt muss die Firewall auch leistungsfähig genug sein, um den Datenstrom ohne große Verzögerungen zu analysieren. Je schneller die Internet-Anbindung, desto mehr Pakete fließen über die Firewall. Soll diese auch die Datenströme – also nicht nur die Pakete, sondern auch den logischen Datenfluss – überwachen, ist ein leistungsfähigeres System erforderlich.

## 1.4.4 Komponenten einer Firewall

Ein Firewall-System kann aus ein bis drei Komponenten bestehen:

- Paketfilterungs-Router
- Proxy-Server (Application Level Gateway)
- Verbindungs-Gateway (Circuit Level Gateway)




**Firewall-Konfiguration:** Hier mit Paketfilterungs-Router und einem Proxy-Server.

Grundsätzlich konkurrieren zwei Firewall-Konzepte: die „passive" Paketfiltertechnologie und die „aktiven" Application Level Gateways. Alle anderen Firewall-Systeme sind Varianten und Weiterentwicklungen dieser beiden Konzepte oder werden damit kombiniert. Dazu gehören etwa das Stateful Packet Filtering, Circuit Level Gateways oder so genannte Hybrid-Firewalls. Diese neueste Variante stellt eine Kombination aus Paketfilter und Application Level Gateway dar.

## 1.4.5 Paketfilterungs-Router

Ein Paketfilterungs-Router entscheidet bei jedem Datenpaket anhand festgelegter Filterregeln, ob er es weiterleitet oder nicht. Überprüft werden Header-Informationen wie:

- IP-Ursprungsadresse
- IP-Zieladresse
- das eingebettete Protokoll (TCP, UDP, ICMP oder IP Tunnel)
- TCP/UDP-Absender-Port
- TCP/UDP-Ziel-Port
- ICMP Message Type

- Eingangsnetzwerkschnittstelle (Ethernet-Karte, Modem et cetera)
- Ausgangsnetzwerkschnittstelle

Falls das Datenpaket die Filter passiert, sorgt der Router für die Weiterleitung des Pakets, andernfalls verwirft er es. Wenn keine Regel greift, verfährt der Paketfilterungs-Router nach den Default-Einstellungen.

Anhand der Filterregeln kann ein Router auch eine reine Service-Filterung durchführen. Auch hier muss der Systemadministrator die Filterregeln vorher definieren. Service-Prozesse benutzen bestimmte Ports (Well Known Ports), wie zum Beispiel FTP den Port 21 oder SMTP den Port 25. Um beispielsweise den SMTP-Service abzublocken, sondert der Router alle Pakete aus, die im Header den Zielport 25 eingetragen haben oder die nicht die Ziel-IP-Adresse eines zugelassenen Hosts besitzen. Einige typische Filter-Restriktionen sind:

- Nach außen gehende Telnet-Verbindungen sind nicht erlaubt.
- Telnet-Verbindungen sind nur zu einem bestimmten internen Host erlaubt.
- Nach außen gehende FTP-Verbindungen sind nicht erlaubt.
- Pakete von bestimmten externen Netzwerken sind nicht erlaubt.

### 1.4.6 Abwehr von Angriffen

Bestimmte Angriffstypen verlangen eine vom Service unabhängige Filterung. Diese ist aber schwierig umzusetzen, da die dazu erforderlichen Header-Informationen Service-unabhängig sind. Die Konfiguration von Paketfilterungs-Routern kann auch gegen diese Art von Angriffen erfolgen. Für die Filterregeln sind jedoch zusätzliche Informationen notwendig. Typische Beispiele dafür liefern Attacken mittels Source IP Address Spoofing, Source Routing oder Tiny Fragments.

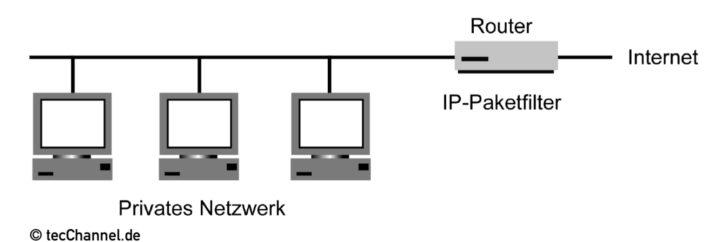
Bei einer Spoofing-Attacke fälscht der Angreifer die IP-Absenderadresse eines Datenpakets und verwendet stattdessen die Adresse eines Rechners im internen Netz. Die Firewall kann einen solchen Angriff erkennen, indem sie überprüft, ob ein von außen kommendes Paket eine interne Adresse nutzt. Um den Angriff abzuwehren, sind solche Pakete entsprechend herauszufiltern.

Bei einer Source-Routing-Attacke gibt der Angreifer die konkrete Route vor, die ein Datenpaket nehmen soll, um Sicherheitsmaßnahmen zu umgehen. Das Verfahren zum Source Routing ist zwar im TCP/IP-Standard vorgesehen, kommt jedoch kaum noch zum Einsatz. Deshalb kann die Firewall die Pakete mit diesem Flag bedenkenlos verwerfen.Tiny Fragment Attacke

Bei Tiny-Fragment-Angriffen erzeugt der Hacker extrem kleine Datenpakete, von denen nur das erste den TCP-Header enthält. Das soll den Router veranlassen, nur das erste Fragment zu prüfen und die restlichen ungeprüft durchzulassen. Dies erlaubt dem Hacker, die gewünschten Befehle ins Netz zu schmuggeln. Als Abwehr kann die Firewall alle Pakete verwerfen, bei denen das Feld Fragment-Offset auf eins gesetzt ist.

### 1.4.7 Vorteile von Paketfilterungs-Routern

Die Mehrzahl der Firewall-Systeme setzen nur einen Paketfilterungs-Router ein. Außer der Zeit, die für die Planung der Konfiguration des Routers erforderlich ist, entstehen keine weiteren Kosten, denn die Filter-Software ist Bestandteil der Router-Software. Um den Datenverkehr zwischen privatem und öffentlichem Netz nicht zu stark einzuschränken, sind von Haus aus nur sehr moderate und wenige Filter definiert. Die Paketfilterung ist im Allgemeinen durchlässig für Benutzer und Applikationen. Sie erfordert zudem kein spezielles Training und keine zusätzliche, auf den einzelnen Rechnern installierte Software.




**Einfache Sicherung:** Hier schützt nur ein Paketfilterungs-Router das Netzwerk.

### 1.4.8 Nachteile

Doch die Paketfilterung hat auch Nachteile. So ist neben detaillierten Protokollkenntnissen für eine komplexe Filterung auch eine lange Regelliste notwendig. Derartige Listen sind sehr aufwendig und daher schwer zu verwalten. Es ist zudem schwierig, die Filter auf Wirksamkeit zu testen. Auch sinkt der Router-Durchsatz, wenn zu viele Filter definiert sind.

Daneben können Hacker die Firewall durch Tunneln der Pakete überwinden, wobei ein Paket vorübergehend in einem anderen gekapselt wird. Und schließlich: Data-driven-Attacken kann der Router nicht erkennen.

### 1.4.9 Proxy-Server

Ein Proxy-Server (Engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.

Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Webinhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internet-Inhalte. Der Proxy zeigt dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Webdokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf.

Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC – allerdings abhängig vom jeweiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen „unsichtbar" hinter ihm.

## 1.4.10 Vorteile eines Proxy-Servers

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus. Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

## 1.4.11 Bastion-Host

Unter einem Bastion-Host versteht man einen besonders gesicherten Rechner, der wie eine Festung wirken soll. Er schützt die Rechner im privaten Netz vor Angriffen von außen. Wie bei einer Festung gibt es nur einen Ein- und Ausgang, der ständig bewacht ist und bei Bedarf sofort geschlossen werden kann. Die Überwachung des Aus- und Eingangs übernimmt meist ein Router als Paketfilter.

Bastion-Hosts sind von ihrer Art her damit die gefährdetsten Rechner in einer Firewall. Auch wenn sie in der Regel mit allen Mitteln geschützt werden, sind sie das häufigste Ziel eines Angriffs, da ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.

Die Rechner im privaten Netz sind aus dem Internet nicht direkt erreichbar und dadurch unsichtbar. Andersherum ist auch das Internet nur über den Bastion-Host zugänglich. Deshalb ergibt sich für diesen Rechner die logische Grundhaltung: Je einfacher der Bastion-Host aufgebaut ist, desto leichter ist er zu schützen. Denn jeder auf dem Bastion-Host angebotene Dienst kann Software- oder Konfigurationsfehler enthalten.

Bei minimalen Zugriffsrechten sollte der Bastion-Host gerade so viele Dienste anbieten, wie er für die Rolle als Firewall unbedingt braucht. Bastion-Hosts werden in unterschiedlichen Architekturen installiert, wie zum Beispiel als Dual-Homed-Host, in Kombination mit einem Überwachungs-Router.

### 1.4.12 Vorteile eines Bastion-Hosts

Ein Bastion-Host lässt sich so einrichten, dass Dienste nur über eine Authentifizierung abrufbar sind. Zudem kann der Administrator spezielle Bestandteile dieser Dienste komplett abschalten, etwa den PUT-Befehl für FTP-Server.

Die voneinander unabhängigen Proxy-Dienste laufen unter einer unprivilegierten Benutzerkennung in separaten, gesicherten Verzeichnissen, so dass ein Angriff über diese Dienste nur schwer möglich ist.

Alle anderen Dienste wie SMTP oder HTTP sind auf diesem Rechner komplett abgeschaltet und stellen somit keine Sicherheitslücke dar. Bei Bedarf überwacht der Administrator auch den gesamten Datenverkehr, um Angreifer zu erkennen.

### 1.4.13 Nachteile von Bastion-Hosts

Bei bestimmten Diensten, wie etwa Telnet oder FTP, müssen sich die Benutzer zwei Mal einloggen: Zum einen erfolgt die Anmeldung auf dem Proxy des Bastion-Hosts, zum anderen auf dem eigentlichen Server. Darüber hinaus gilt es auch die Client-Software speziell an den Proxy anzupassen.

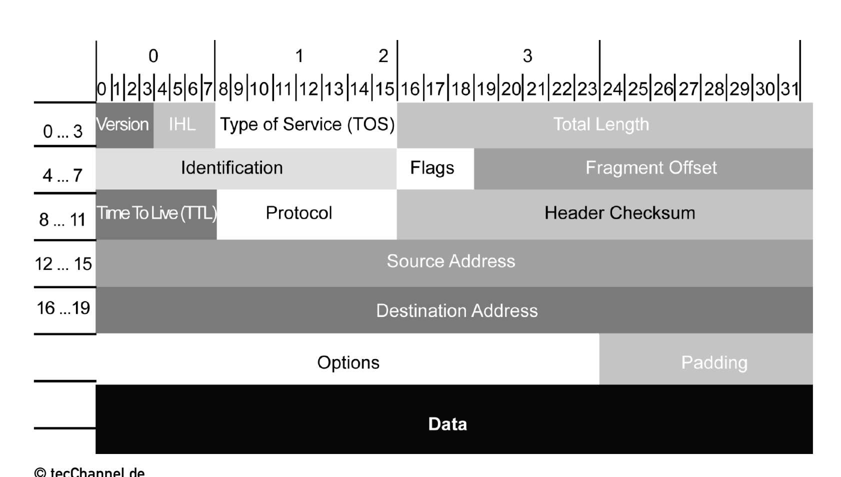
### 1.4.14 Verbindungs-Gateways

Verbindungs-Gateways (Circuit Level Gateways) sind Proxy-Server mit Zusatzfunktionen. Sie beschränken sich, ähnlich wie Application Level Gateways, nicht nur auf die Kontrolle der IP- und Transportschicht-Header. Stattdessen bauen Sie die Datagramme der Transportschicht aus den IP-Paketen, die unter Umständen fragmentiert sind, zusammen.

Wie bei Application Level Gateways existieren auch bei Verbindungs-Gateways keine direkten Verbindungen zwischen der Innen- und Außenwelt. Vielmehr findet automatisch eine Adressübersetzung statt. So lässt sich eine Benutzerauthentifizierung erzwingen.

Andererseits verstehen die Circuit Level Gateways das Anwendungsprotokoll nicht und können deshalb keine Inhaltskontrolle durchführen. Beide Gateway-Varianten verfügen zwar über gemeinsame Merkmale; die Fähigkeit, das Anwendungsprotokoll zu verstehen, besitzt jedoch nur das Application Level Gateway.

Verbindungs-Gateways vertrauen den internen Benutzern. In der Praxis werden Proxy-Server daher für die Verbindungen nach innen benutzt, während man Verbindungs-Gateways für den Datenverkehr von innen nach außen einsetzt.




**IP-Pakete:** Ein Verbindungs-Gateway muss aus den Daten im IP-Header ersehen, welche Pakete zu einem Datenstrom gehören.

## 1.4.15 Hybrid-Firewalls

Hybrid-Firewalls bestehen aus Paketfilter und Application Level Gateway, wobei das Gateway die Filterregeln des Paketfilters dynamisch ändern kann. Als „Stateful Inspection" bezeichnet man einen Paketfilter „mit Gedächtnis". Dieser speichert allerdings nur die Informationen aus den Paket-Headern.

Der Vorteil einer Hybrid-Firewall gegenüber einem alleinigen Application Level Gateway liegt in der höheren Performance. Allerdings bedingt dies auch einen gewissen Sicherheitsverlust, da bei den meisten Protokollen der Proxy nach dem Öffnen der Paketfilter keinerlei Kontrolle über die Verbindung besitzt. Ein Angreifer muss den Proxy nur eine Zeit lang in Sicherheit wiegen und hat anschließend durch den für ihn geöffneten Paketfilter freies Spiel.

Die „Stateful Inspection Engine" analysiert die Datenpakete bei der Übertragung auf Netzwerkebene. Gleichzeitig erstellt sie dynamische Zustandstabellen, die die Betrachtung mehrerer Pakete erlauben. Die Korrelationen zwischen zusammengehörenden ein- und ausgehenden Paketen ermöglichen ausgefeilte Analysen.

## 1.4.16 Hochsicherheits-Firewalls

Hochsicherheits-Firewalls können aus einem Firewall-Subnetz mit zwei Paketfilterungs-Routern und einem Proxy (Bastion Host) bestehen. Ein solches Firewall-System sichert auf der Netzwerk- und Applikationsebene durch die Definition

einer „entmilitarisierten Zone“ (Englisch: demilitarized zone, kurz DMZ). Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. Das DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.

Dabei ist das DMZ so konfiguriert, dass Zugriffe aus dem privaten Netz und dem Internet nur auf Server im DMZ erfolgen können. Direkter Verkehr durch das DMZ-Netz hindurch ist nicht möglich – egal in welcher Richtung. Bei den hereinkommenden Datenpaketen schützt der äußere Router gegen Standard-Angriffe wie IP-Address-Spoofing oder Routing-Attacken und überwacht gleichzeitig den Zugriff auf das DMZ-Netz. Dadurch können externe Rechner nur auf den Bastion-Host und eventuell auf den Information-Server zugreifen.

Durch den internen Router wird eine zweite Verteidigungslinie aufgebaut. Dieses Gerät überwacht den Zugriff vom DMZ zum privaten Netz, indem es nur Pakete akzeptiert, die vom Bastion Host kommen. Damit gelangen nur Benutzer in das interne Netz, die sich vorher am Bastion-Host authentifiziert haben.

## 1.4.17 Fazit

Wer sein Firmennetzwerk an das Internet anschließt, geht ein nicht unerhebliches Risiko ein. Da aber kaum noch eine Firma ohne Internet-Anschluss auskommt, gehört eine Firewall zum Pflichtprogramm. Die Paranoia lässt sich beliebig weit treiben, man muss nur genügend Zeit und Geld investieren.

Jede Firewall ist allerdings nur so gut wie ihre Konfiguration und die Absicherung des Hosts, auf dem sie läuft. Wer einfach das Software-Paket aufspielt oder einen fertigen Firewall-Rechner in sein Netz hängt und sich damit sicher wähnt, handelt fahrlässig. Deshalb ist es oftmals besser, sich an ein auf Netzwerkabsicherung spezialisiertes Unternehmen zu wenden.

Peter Klau

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Test: Sechs Personal Firewalls | a405 | – |
| Linux als Firewall | a695 | – |
| Desktop-Firewall mit Linux 2.4 | a751 | – |
| Linux Firewall mit ipchains | a704 | – |
| Sichere Linux-Workstation | a720 | – |
| Hackerangriffe unter Linux entdecken | a715 | – |
| VPN: Daten sicher übers Internet | a306 | – |
| So funktioniert TCP/IP | a209 | – |
| Die Netzwächter | a600 | – |

# 2. Netzwerk-Sicherheit

Als zentralen Elementen zwischen allen Clients und gegebenenfalls dem Internet sollte dem Netzwerk und den Servern bei der Sicherheitsplanung eine nicht zu geringe Bedeutung beigemessen werden. Im ersten Abschnitt erfahren Sie alles über wichtige, unwichtige und gefährliche TCP/IP-Ports. Wie Sie Ihren E-Mail-Server gegen Spam schützen, zeigt der zweite Beitrag. Eine Anleitung zum wasserdichten Versiegeln ihres Wireless LAN schließt das Kapitel ab.

## 2.1 Ports im Überblick

Ohne Ports wäre eine Kommunikation über die im Internet üblichen Protokolle Transmission Control Protocol (TCP) und User Datagram Protocol (UDP) nicht möglich. Die Nebenstellen erlauben es, dass mehrere Anwendungsprozesse über eine Internet-Verbindung gleichzeitig Daten austauschen können.

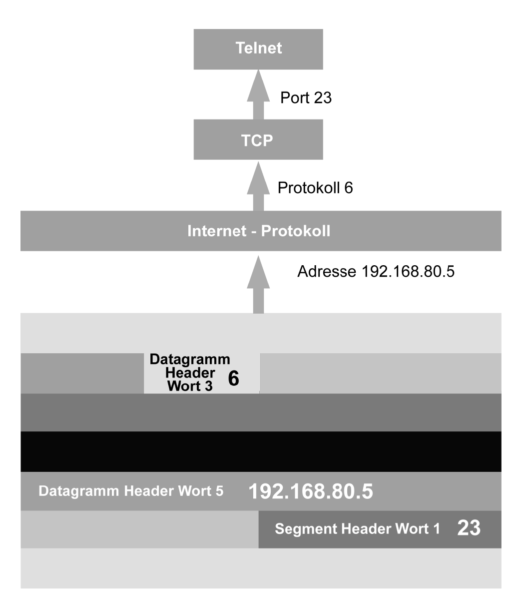
Auch bei der Konfiguration einer Firewall ist ein Grundwissen über Portnummern von Nöten. Ein Paketfilter entscheidet bei jedem Datenpaket anhand festgelegter Filterregeln, ob er es weiterleitet oder nicht. Dabei werden unter anderem Header-Informationen wie Absender- und Zielport ausgelesen. Auf Grund dieser Regeln kann eine Firewall reine Service-Filterungen vornehmen.

Service-Prozesse benutzen immer bestimmte Ports. Um beispielsweise den FTP-Service abzublocken, sondert die Firewall alle Pakete aus, die im Header den Port 21 eingetragen haben. Ebenso spielt es eine große Rolle, von welchem Rechner aus eine Verbindung aufgebaut wird: von einem Client im LAN oder von einem externen Rechner.

In diesem Beitrag erläutern wir Ihnen die Funktionsweise von Ports und welche verschiedenen Gruppen es gibt. Darüber hinaus haben wir für Sie eine Übersicht über die wichtigsten Firewall-Regeln für ein Firmennetz zusammengestellt, die wir in regelmäßigen Abständen ergänzen. In unserer tecDaten-Tabelle (**webcode: d901**) finden Sie zudem zahlreiche Informationen zu „guten und bösen“ Programmen, die Ports nutzen.

### 2.1.1 Was sind Portnummern?

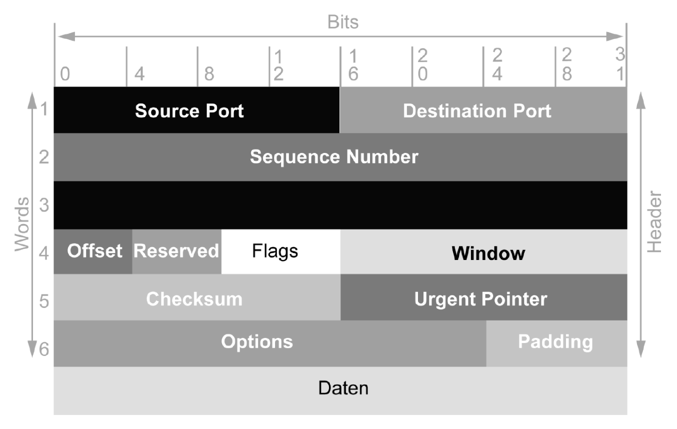
Portnummern zählen zu den grundlegenden Elementen beim Einsatz der Protokolle TCP und UDP. Sind die Daten am Zielrechner angekommen, müssen sie noch an den richtigen Anwendungsprozess ausgeliefert werden. Beim Transport der Informationen durch die Netzwerkschichten benötigt man einen Mechanismus, der zuerst einmal die Übergabe an das jeweilige richtige Protokoll sicherstellt.




© tecChannel.de

**Nebenstellen:** Nach Empfang der Daten werden diese an den richtigen Anwendungsprozess übergeben.

Das Zusammenlegen von Daten aus mehreren Quellen zu einem einzigen Datenstrom nennt man Multiplexen. Ankommende Daten aus dem Netz muss das Internet Protocol (IP) also demultiplexen. Dazu kennzeichnet das IP die Transportprotokolle mit Protokollnummern. Die Transportprotokolle selber nutzen wiederum die Portnummern zur Identifizierung von Anwendungen.




© tecChannel.de

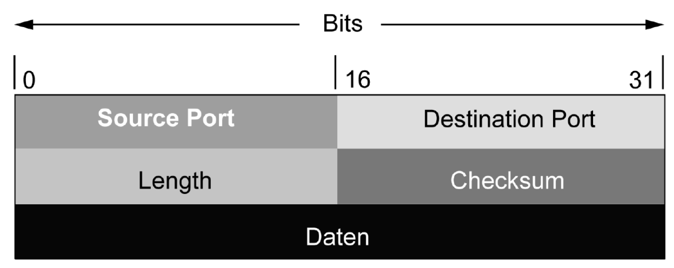
**TCP-Header:** Die 16 Bit lange „Destination Port"-Nummer legt fest, für welche Applikation das Datenpaket bestimmt ist.

Die IP-Protokollnummer steht in einem Byte im dritten Wort des Datagramm-Headers. Dieser Wert bestimmt die Übergabe an das jeweilige Protokoll in der Transportschicht, beispielsweise „6“ für TCP oder „17“ für UDP. Das Transportprotokoll muss nach dem Empfang die Daten an den richtigen Anwendungsprozess übergeben.

Anwendungsprozesse werden anhand der 16 Bit langen Portnummer identifiziert, an die die Daten nach Empfang auf dem Zielrechner übergeben werden. Im ersten Wort jedes TCP- und UDP-Headers sind daher sowohl die „Source Port“-Nummer als auch die „Destination Port“-Nummer enthalten. Soll also eine Applikation unter einer bestimmten Portnummer erreichbar sein, teilt sie dies dem TCP/IP-Protokoll-Stack mit.

## 2.1.2 Sockets

Die Kombination aus IP-Adresse und Portnummer bezeichnet man als Socket. Damit ist es möglich, einen einzelnen Netzwerkprozess innerhalb des gesamten Internets eindeutig zu identifizieren. Die Notation ist folgende: IP-Adresse:Port, zum Beispiel 62.96.227.70:80. Zwei Sockets definieren eine Verbindung: einer für den Ausgangs- und einer für den Zielrechner.




© tecChannel.de

**User Datagram Protocol:** Der minimale Protokollmechanismus des UDP enthält ebenfalls den Zielport des Datenpakets.

TCP und UDP können dieselben Portnummern vergeben. Erst die Kombination aus Protokoll und Portnummer ist eindeutig. Somit ist die Portnummer 53 in TCP nicht identisch mit der Portnummer 53 in UDP.

Den Aufbau und die Funktionsweise der Protokollfamilie TCP/IP erläutern wir Ihnen ausführlich im tecCHANNEL-Beitrag „So funktionieren TCP/IP und IPv6“ (**webcode: a209**).

### 2.1.3 Portgruppen

Insgesamt stehen jeweils 65.535 verschiedene TCP- und UDP-Ports zur Verfügung. Um einen Überblick zu behalten und bestimmten Applikationen feste Nummern zuweisen zu können, hat man diese in drei Gruppen unterteilt:

Well Known Ports: Bei diesem Typ handelt es sich um reservierte und standardisierte Portnummern zwischen 1 und 1023. Dies vereinfacht den Aufbau einer Verbindung, weil Absender und Empfänger bereits wissen, dass Daten für einen bestimmten Prozess an einen bestimmten Port gesendet werden müssen. So nutzen beispielsweise alle Telnet-Server den Port 23.

Die Well Known Ports ermöglichen den Clients die Verbindung zu Servern, ohne dass eine weitere Konfiguration notwendig ist. Die Verwaltung dieser Ports übernimmt die Internet Assigned Numbers Authority (IANA). Eine Liste der aktuell vergebenen Portnummern finden Sie unter der Adresse www.iana.org/assignments/port-numbers.

Bis 1992 bewegten sich die Well Known Ports im Bereich zwischen 1 und 255. Die Nebenstellen zwischen 256 und 1023 wurden für Unix-spezifische Dienste verwendet.

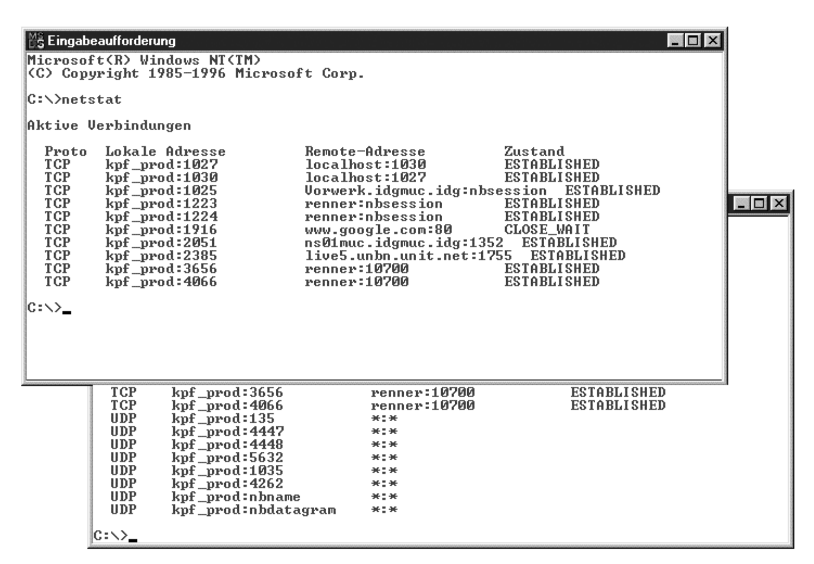
Registered Ports: Diese Ports im Bereich von 1024 bis 49.151 sind für Dienste vorgesehen, die üblicherweise auf bestimmten Nebenstellen laufen. Ein Beispiel hierfür ist der Port 3128, der von Proxy-Servern oft alternativ für das Hypertext Transport Protocol (HTTP) verwendet wird.

Dynamically Allocated Ports: Diese auch Ephemeral Ports genannten Nebenstellen werden stets dynamisch zugewiesen. Sie liegen im Bereich von 49.152 bis 65.535. Jeder Client kann diese Ports nutzen, solange die Kombination aus Transportprotokoll, IP-Adresse und Portnummer eindeutig ist. Wenn ein Prozess einen Port benötigt, fordert er diesen bei seinem Host an.

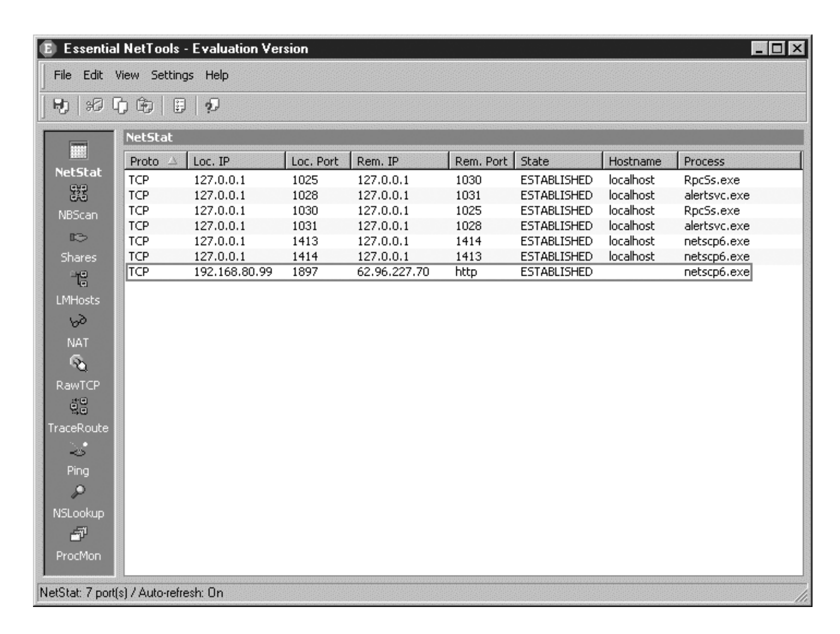
### 2.1.4 Welcher Port wird verwendet?

Wie bereits erwähnt, ist für die Einrichtung einer Firewall das Wissen über Ports unerlässlich. Sie müssen festlegen, von welchen Nebenstellen Verbindungen ein- und ausgehen dürfen. Doch oft weiß man nicht, welche Ports eine Applikation benutzt. Oder man möchte nachsehen, welche Nebenstelle für ein Programm auf dem Client gerade dynamisch nach dem Zufallsprinzip zugewiesen wurde.

Um dies herauszufinden, können Sie beispielsweise das Windows-Bordmittel Netstat verwenden. Allerdings hat dieses Tool nur einen geringen Funktionsumfang. So zeigt das Programm nicht an, welche Verbindung von welcher Applikation verwendet wird.




**Microsoft Netstat:** Das Tool bietet nur wenige Details zu offenen Verbindungen.



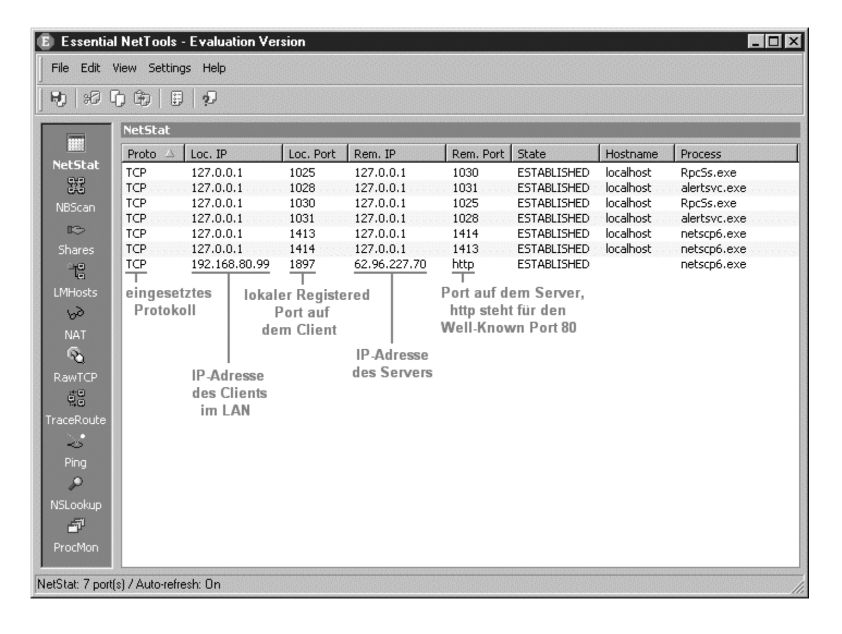

| Proto | Loc. IP | Loc. Port | Rem. IP | Rem. Port | State | Hostname | Process |
|---|---|---|---|---|---|---|---|
| TCP | 127.0.0.1 | 1025 | 127.0.0.1 | 1030 | ESTABLISHED | localhost | RpcSs.exe |
| TCP | 127.0.0.1 | 1028 | 127.0.0.1 | 1031 | ESTABLISHED | localhost | alertsvc.exe |
| TCP | 127.0.0.1 | 1030 | 127.0.0.1 | 1025 | ESTABLISHED | localhost | RpcSs.exe |
| TCP | 127.0.0.1 | 1031 | 127.0.0.1 | 1028 | ESTABLISHED | localhost | alertsvc.exe |
| TCP | 127.0.0.1 | 1413 | 127.0.0.1 | 1414 | ESTABLISHED | localhost | netscp6.exe |
| TCP | 127.0.0.1 | 1414 | 127.0.0.1 | 1413 | ESTABLISHED | localhost | netscp6.exe |
| TCP | 192.168.80.99 | 1897 | 62.96.227.70 | http | ESTABLISHED | | netscp6.exe |

**Essential NetTools:** Die Shareware-Alternative zum Windows-Bordmittel enthält ausführliche Informationen zu offenen Ports und Verbindungen.

Empfehlenswerter ist die Shareware Essential NetTools (http://www.tamos.com/products/nettools/) von Tamos Software. Eines der Features ist das sehr ausführliche Netstat-Tool. Es zeigt nicht nur die offenen Ports und Verbindungen auf einem System an, sondern zusätzlich auch eine Klartext-Auflösung der Adressen und Nebenstellen sowie die dazugehörige Applikation inklusive dem kompletten Pfad.

### 2.1.5 Beispiel für eine Verbindung

In diesem Beispiel laden wir mit einem Webbrowser eine Internet-Seite von www.tecChannel.de herunter. Der Browser baut dabei eine Verbindung zu der IP-Adresse 62.96.227.70 auf. Auf dem Server wird der TCP-Port 80 verwendet, der Well Known Port für Webserver. Auf dem Client läuft die Verbindung über die dynamische Nebenstelle 1897.




**Beispiel für eine Verbindung:** Der Webbrowser, hier Netscape 6.2, lädt eine Internet-Seite von www.tecChannel.de herunter.

Der Client, der die Internet-Seite abruft, liegt in einem lokalen Netzwerk, erkennbar an der IP-Adresse 192.168.80.99. Die Daten laufen über einen Router und über Network Address Translation (NAT) kommt Masquerading zum Einsatz.

### 2.1.6 Router: Masquerading

Wenn der Internet-Zugang über einen Router mit dem Internet erfolgt, so ist eine direkte Port-zu-Port-Kommunikation unter TCP/IP nicht möglich.

Meist werden in lokalen Netzwerken private IPv4-Adressen verwendet, da die Zuteilung von offiziellen IPv4-Adressen in größeren Mengen mittlerweile schwierig geworden ist. Der gesamte Internet-Traffic läuft über einen Router. Mit einer solchen Absenderadresse können Clients jedoch nicht direkt mit dem Internet in Kontakt treten. Die Antwortpakete finden den Weg nicht zurück. Woher kennt nun ein Server im Internet die entsprechende Portnummer eines Clients im LAN?

Hier kommt das so genannte Masquerading zum Einsatz. Dabei handelt es sich um eine spezielle Art der Adressumsetzung, welche auch Source Network Address Translation (SNAT) genannt wird. Bei Paketen von intern, die über den Router nach extern gelangen sollen, wird die Quelladresse durch die des Routers und der ursprüngliche Quellport durch eine neue Nebenstelle ersetzt. Diese Daten werden in einer Tabelle hinterlegt, damit die Antwortpakete wieder entsprechend umgesetzt werden können. So „merkt“ ein Internet-Service nicht, dass er mit einem Port des Routers kommuniziert statt mit dem Client.

Weitere Details zu Masquerading erfahren Sie im tecCHANNEL-Beitrag „Masquerading mit Linux“ (**webcode: a707**).

### 2.1.7 Router: Port-Forwarding

Durch das Funktionsprinzip von Network Address Translation (NAT), wie es in vielen Firmennetzen eingesetzt wird, ist es nicht möglich, von außen direkte Verbindungen zu einem Rechner hinter einem Router aufzubauen. Als Port-Forwarding oder Port-Mapping bezeichnet man die Technik, bei der ein Rechner auf einem bestimmten Port auf einen Verbindungsaufbau wartet und die Datenpakete an einen anderen Computer im LAN weiterleitet. Damit ist der Betrieb eines Internet-Servers auf einem Client hinter einem Router möglich.

Zugegriffen wird somit nicht direkt auf den Rechner im lokalen Netz, sondern auf einen bestimmten Port des Routers. Dieser leitet den Zugriff auf den entsprechenden Port des Zielrechners weiter. Die Pakete, die der Rechner zurückschickt, müssen ebenfalls bearbeitet werden. Es werden die IP-Adresse und die Portnummer des Rechners durch die IP-Adresse und den Forwarding-Port auf dem Router ersetzt. Port-Forwarding ist sozusagen ein Gegenstück zum Masquerading. Wie bei diesem sind die Clients für das Internet unsichtbar.

Zum besseren Verständnis hier ein Beispiel, wie Port-Forwarding für einen Webserver ablaufen könnte: Ein Client mit der Adresse 192.168.80.99 in einem lokalen Netz ist über einen Router mit der öffentlichen Adresse 194.246.96.76 mit dem Internet verbunden. Um auf den Webserver auf dem Client zugreifen zu können, wird der Router dahingehend konfiguriert, dass er sämtliche Datenpakete für

den Port 4711 an den Port 80 auf dem Rechner 192.168.80.99 weiterleitet. Die Antwortpakete von 192.168.80.99:80 werden also vom Router auf 194.246.96.76: 4711 umgeschrieben.

## 2.1.8 Ports – ein offenes Tor

Die TCP- und UDP-Ports können jedoch auch ein Sicherheitsrisiko darstellen. Zahlreiche Würmer und Trojaner greifen über diese auf lokale Systeme zu oder bauen eine Verbindung ins Internet auf. Gerade unter Windows-Systemen ist daher der Einsatz einer Firewall anzuraten.

In bestimmten Kreisen entwickelt es sich mittlerweile zum Volkssport, wahllos IP-Adressen auf Backdoors zu untersuchen und sich damit unbemerkt Zugang zu verschaffen. Mit Hilfe eines Portscanners können Angreifer sehr schnell herausfinden, welche Ports auf einem Rechner offen sind. Ein solcher Scanner macht dabei nichts anderes, als alle Nebenstellen einzeln abzuklappern und zu prüfen, ob dort eine Antwort kommt. Wenn sie kommt, ist der entsprechende Port aktiv und kann möglicherweise missbraucht werden.

Aus diesem Grund ist der Einsatz einer Firewall unerlässlich. Im nächsten Abschnitt erläutern wir Ihnen die Konfiguration einer Firewall anhand von Regeln. Wenn Sie diese auf Ihrem Rechner anwenden, sind Sie vor den meisten Gefahren im Internet geschützt. Grundlagen und weitere Infos über die Funktionsweise einer Firewall erfahren Sie im tecCHANNEL-Beitrag „Firewall-Grundlagen“ (**webcode: a682**).

## 2.1.9 Einrichten einer Firewall

Im Folgenden erläutern wir Ihnen anhand einer Meta-Sprache wichtige Filterregeln für eine sichere Firewall. Diese lassen sich auf alle üblichen Firewalls anwenden. Grundsätzlich sollte man alle Ports erst einmal sperren und nur die öffnen, die wirklich benötigt werden. Filterregeln ergeben sich aus mehreren Optionen, die in folgender Tabelle aufgeführt werden:

**Firewall-Optionen**

| Option | Beschreibung |
|---|---|
| FORWARD/ACCEPT/ REJECT/DROP | Datenpakete weiterleiten/annehmen/ blockieren/ignorieren |
| -dir IN/OUT | Eingehend/ausgehend |
| -prot TCP/UDP/ICMP | Verwendetes Protokoll: TCP, UDP oder ICMP |
| -src HOST:PORT | Quellrechner:Port |
| -dest HOST:PORT | Zielrechner:Port |

```
FORWARD/ACCEPT/REJECT/DROP -dir IN/OUT -prot TCP/UDP -src
HOST:PORT -dest HOST:PORT
```

Über die IP-Adresse des Quellrechners können Sie Dienste für bestimmte Rechner in Ihrem lokalen Netz sperren. Zudem sollte man bei der Konfiguration beachten, dass einige Dienste nicht über eine bereits geöffnete Datenverbindung antworten, sondern eine neue Verbindung aufbauen. Aus diesem Grund sollte die Firewall auch fallweise Verbindungen erlauben:

```
IF FORWARD/ACCEPT/REJECT/DROP -dir IN/OUT -prot TCP/UDP -src
HOST:PORT -dest HOST:PORT THEN FORWARD/ACCEPT/REJECT/DROP -
dir IN/OUT -prot TCP/UDP -src HOST: PORT -dest HOST:PORT
```

Mehrere einzelne Regeln nennt man auch Ruleset. Bei jeder Anfrage aus dem lokalen Netz oder aus dem Internet wird das Ruleset von oben bis unten abgearbeitet. Es verarbeitet und filtert jedes Datenpaket.

In unserem Konfigurationsbeispiel sind in einer Firma mehrere Clients über eine Firewall mit dem Internet verbunden. Ein Proxy-Server wird nicht eingesetzt.

## 2.1.10 Standarddienste: FTP

Im ersten Schritt empfiehlt es sich, die Standarddienste zu konfigurieren, die in der Regel bei den meisten Internet-Verbindungen benötigt werden. Hierzu zählt unter anderem der Zugriff auf Webseiten und FTP-Server.

Domain Name Service: Diese Regel ermöglicht es dem lokalen Rechner, eine Verbindung mit dem Nameserver des Providers aufzubauen. Diese beiden Regeln werden in jedem Fall benötigt:

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
53
```

```
FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:
53
```

Weitere Details zum Domain Name System erfahren Sie im entsprechenden tecCHANNEL-Beitrag (**webcode: a205**).

File Transfer Protocol: Das FTP bietet zwei verschiedene Verbindungsarten, die unterschiedliche Portfiltereigenschaften voraussetzen. Grundsätzlich sollte man dem passiven FTP den Vorzug geben, da hier alle Verbindungen vom Client aus aufgebaut werden und keine von außen initiierten Verbindungen zugelassen werden müssen. Im aktiven Modus baut der Client eine Verbindung zum Port 21 des Servers auf. Der Server bestätigt die Verbindung und baut eine Verbindung von

seinem Port 20 zum Client auf. Der Vollständigkeit halber erläutern wir jedoch beide Varianten. Beim aktiven FTP sollte die Firewall dahingehend konfiguriert werden, dass nur der Server eine Verbindung aufbauen darf, zu dem zuvor der entsprechende Client eine Verbindung über Port 20 aufgebaut hat.

Passives FTP:

```
FORWARD -dir OUT -prot TCP -scr LOCAL_CLIENT:ANY ANY:21
```

Aktives FTP:

```
IF FORWARD -dir OUT -prot TCP -scr LOCAL_CLIENT:ANY FTP_SER-
VER:21 THEN FORWARD -dir IN -prot TCP -src FTP_SERVER:20 LO-
CAL_CLIENT:ANY
```

## 2.1.11 Standarddienste: SSH und HTTP

SSH Remote Login Protocol: SSH ermöglicht eine sichere Kommunikation und Authentifizierung. Dazu wird der komplette Login-Prozess einschließlich der Passwortübermittlung verschlüsselt. Diese Regel sollte man nur bei Bedarf einrichten.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
22
```

Hypertext Transfer Protocol: HTTP ist das Standardprotokoll für Webbrowser und ermöglicht den Zugriff auf Internet-Seiten.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
80
```

Wenn im Firmennetz ein Proxy-Server zum Einsatz kommt, muss die Regel entsprechend angepasst werden.

Hypertext Transfer Protocol over TLS/SSL: Dient zur sicheren Übertragung von Webseiten zwischen Webserver und Browser. Die Kommunikation erfolgt hierbei SSL-verschlüsselt. Das HTTPS-Protokoll wird von zahlreichen Webseiten verwendet, wie beispielsweise beim Online-Banking. Daher sollten die entsprechenden Ports freigegeben werden.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
443
```

## 2.1.12 Mail- und Newsdienste

Damit ein Zugriff auf externe Mailserver zum Senden und Empfangen von Mails möglich ist, müssen auch hier entsprechende Ports freigegeben werden.

Simple Mail Transfer Protocol: Das SMTP wird in der Regel zum Versenden von Nachrichten verwendet. Soll der Versand von Mails nur über einen bestimmten Server möglich sein, so kann man dies hier festlegen. Nachrichten lassen sich so beispielsweise nur über den Firmen-Mailserver verschicken.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
25
```

Post Office Protocol Version 3: Diese Regel ermöglicht das Abrufen von Mails von POP3-Mailservern. Auch hier besteht die Möglichkeit, den Zugriff wieder auf bestimmte Server zu beschränken.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
110
```

Network News Transfer Protocol: NNTP dient zur Übertragung von Usenet-Nachrichten. Diese Regel sollte nur bei Bedarf angelegt werden.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
119
```

Internet Message Access Protocol Version 4: Soll der Zugriff auf E-Mails über IMAP4 erfolgen, so muss man hierfür ebenfalls eine Regel anlegen.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
143
```

Internet Message Access Protocol Version 4 over TLS/SSL: Dieses Protokoll dient der SSL-verschlüsselten Datenübertragung zwischen Mail-Client und IMAP4-Server. Diese Regel ist nur anzulegen, sofern das Protokoll eingesetzt wird.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
993
```

Post Office Protocol Version 3 over TLS/SSL: Falls der verwendete POP3-Server eine sichere Datenübertragung über SSL unterstützt, ist folgende Paketfilterregel anzulegen:

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
995
```

Weitere Informationen zu den Protokollen SMTP, POP und IMAP sowie zu der grundlegenden Technik und zum Aufbau einer E-Mail erfahren Sie im tecCHANNEL-Beitrag „So funktioniert E-Mail“ (**webcode: a819**).

## 2.1.13 Audio und Video: Realplayer

In diesem Abschnitt erfahren Sie, welche Paketfilterregeln nötig sind, um häufig eingesetzte Audio- und Video-Programme wie Apples QuickTime-Player oder den RealPlayer mit einer Firewall einsetzen zu können. Diese Regeln sollten nur dann angelegt werden, wenn es unbedingt sein muss. Ist dies der Fall, ist es ratsam, die Regeln nur für bestimmte Clients im LAN freizugeben.

Real Player: Der Player baut über die TCP-Ports 554, 7070 und 7071 eine Verbindung zum entsprechenden Streaming-Server auf. Den Audio-/Video-Stream sendet der Server von einem der UDP-Ports zwischen 6970 und 7170. Da es aber nicht ratsam ist, alle diese Ports freizugeben, empfehlen wir, nur einen UDP-Port für den Real Player freizugeben und in der Software diesen einen Port einzutragen. Alternativ kann man den Stream auch über TCP empfangen. Die Qualität soll jedoch laut Real schlechter sein.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
554

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
7070

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
7071
```

Der UDP-Port sollte zwischen 6970 und 6997 liegen, da diese derzeit noch keine Registered Ports sind, zum Beispiel:

```
IF FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY REAL_
SERVER:554 THEN FORWARD -dir IN -prot UDP -src REAL_SERVER:
6971 -dest LOCAL_CLIENT:ANY
```

Die Firewall sollte dahingehend konfiguriert werden, dass nur der Server eine Verbindung aufbauen darf, zu dem zuvor der entsprechende Client eine Verbindung aufgebaut hat.

## 2.1.14 Audio und Video: Mediaplayer

Microsoft Media Player: Der Media Server verwendet für Audio- und Video-Streams (*.asf) ein proprietäres Serverprotokoll, das von Microsoft entwickelt wurde. Dieses wird vom MS Media Server ab Version 4.0 sowie vom MS Media Player unterstützt. Der Media Player kontaktiert zum Verbindungsaufbau den Server auf dem TCP-Port 1755. Der Stream wird dann über den UDP-Port 1755 vom Server zum Client gesendet.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
1755
```

```
IF FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY MEDIA_
SERVER:1755 THEN FORWARD -dir IN -prot UDP -src MEDIA_SER-
VER:1755 -dest LOCAL_CLIENT:ANY
```

Apple QuickTime: Der Audio-/Video-Player verwendet für den Verbindungsaufbau zum Server wie der Real Player den TCP-Port 554. Die Streaming-Daten sendet Apples QuickTime-Player über die UDP-Ports 6970 bis 6999 zum Client. Auch hier ist es nicht empfehlenswert, alle diese Nebenstellen freizugeben. In diesem Fall raten wir, den QuickTime-Stream über HTTP zu empfangen.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
554
```

## 2.1.15 Kommunikation und Chat

In der Regel haben Instant Messenger in einem Firmennetz nichts verloren. Soll es dennoch möglich sein, sie einzusetzen, erfordert dies eigene Filterregeln.

ICQ: Für die Client-zu-Server-Kommunikation mit dem Rechner „login.icq.com" verwendet das Programm den TCP-Port 5190. Optional kann für diesen Server auch der TCP-Port 443 mit SSL-Verschlüsselung verwendet werden. Zur Kommunikation zwischen den Clients kommen beliebige TCP-Ports zwischen 1024 und 65535 zum Einsatz. Hier sollte man nur einen Port freigeben und diesen in den Optionen von ICQ festlegen.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest
login.icq.com:5190
```

Yahoo! Messenger: Bei diesem Messenger läuft die gesamte Kommunikation über den TCP-Port 5050. Daher kommen folgende drei Server zum Einsatz: „cs1.yahoo.com", „cs2.yahoo.com" sowie „cs3.yahoo.com". Daher sind für diese

drei Server die Ports freizugeben. Kann über den Port 5050 keine Verbindung zum Yahoo!-Server hergestellt werden, wird der Port 80 verwendet.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY
cs1.yahoo.com:5050

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY
cs2.yahoo.com:5050

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY
cs3.yahoo.com:5050
```

AOL Instant Messenger: AOLs Chat-Programm verwendet wie ICQ den TCP-Port 5190.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
5190
```

MSN Messenger: Microsofts Instant Messenger nutzt zur Kommunikation den TCP-Port 1863. Zur Verwendung der „AOL Instant Messenger"-Integration muss zusätzlich der TCP-Port 5190 freigegeben werden:

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
1863
```

AIM-Integration:

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
5190
```

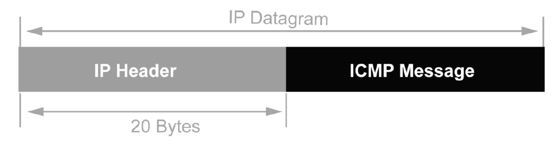
## 2.1.16 ICMP: Internet Control Message Protocol

Das Internet Control Message Protocol (ICMP) dient zum Austausch von Fehler- und Statusmeldungen, falls bei der Übertragung des Internet Protocol (IP) Fehler auftreten. Ist beispielsweise ein Host nicht erreichbar, sendet ein Router die Fehlermeldung „Destination Unreachable" zum Absender. Neben der Fehlerübermittlung dient ICMP auch zur Kontrolle: So verwendet der Ping-Befehl ICMP-Pakete, um die Laufzeit von Datagrammen zwischen zwei Hosts zu ermitteln.

Weitere Details zum Thema Internet Control Message Protocol (ICMP) finden Sie darüber hinaus auf tecCHANNEL.de im Beitrag „So funktionieren TCP/IP und IPv6" (**webcode: a209**).

Bits: 0, 4, 8, 12, 16, 20, 24, 28, 31

| Words | | | | | Header |
|---|---|---|---|---|---|
| 1 | Version | IHL | TYPE Of Service | Total Length | |
| 2 | Identification Number | | Flags | Fragment Offset | |
| 3 | Time To Live | Protocol | IP Header Checksum | | |
| 4 | IP Source Address | | | | |
| 5 | IP Destination Address | | | | |
| 6 | ICMP Data | | | | |




© tecChannel.de

**Bit für Bit:** ICMP-Header und -Datagramm im Detail.

## 2.1.17 Angriffe über ICMP

Das Internet Control Message Protocol ist eine Gratwanderung zwischen Sicherheit und Performance. Wer geringe Performance-Einbußen in Kauf nimmt, kann das Protokoll vollständig blocken. Die Internet-Verbindung sollte in den meisten Fällen trotzdem problemlos funktionieren.

Die Gefahr ist, dass das ICMP für Angriffe missbraucht werden kann, indem künstlich falsche Fehlermeldungen versendet werden. So ist beispielsweise ein Angriff wie Denial-of-Service (DoS) möglich. Ein solcher Angriff kann zum Ausfall von Diensten oder sogar zum Systemabsturz eines Rechners führen.

Durch die ICMP-Dienste Echo und Echo Reply kann sich ein Angreifer auch nützliche Informationen über den Aufbau eines Netzwerks verschaffen. Hierzu gehören die Anzahl der Maschinen und deren IP-Adressen. Diese Informationen können von Hackern dann für weitere, gezielte Angriffe verwendet werden.

Weitere Details zu möglichen Angriffen aus dem Internet bietet Ihnen der Artikel „Firewall-Grundlagen“ (**webcode: a682**).

## 2.1.18 ICMP-Meldungen

Wie bereits erwähnt, sollte man grundsätzlich erst einmal alle Ports schließen und nur diejenigen öffnen, die wirklich benötigt werden. Bei ICMP gibt es zahlreiche Meldungen, in der Praxis braucht man jedoch nur wenige. Die Meldungen sind in ICMP-Typen unterteilt. Weitere Informationen zu den einzelnen Typen finden Sie auf den Webseiten der IANA (www.iana.org/assignments/icmp-parameters). Die benötigten Paketfilterregeln erläutern wir Ihnen im Folgenden.

## 2.1.19 Fehlermeldungen

Typ 3 – Destination Unreachable : Diese Meldung wird versendet, falls ein Gateway ein entsprechendes Netz oder ein Zielrechner ein Protokoll oder einen Port nicht finden kann. Eingehende Datenpakete dieses Typs sollte man zulassen. Dies spart Wartezeit, ansonsten muss der Client auf einen Time-out warten.

```
FORWARD -dir IN -prot ICMP_Typ_3 -src ANY:ANY -dest LOCAL_
CLIENT:ANY
```

Typ 11 – Time Exceeded: Dem Sender eines Datenpakets teilt diese Meldung mit, dass das Datenpaket wegen einer Zeitüberschreitung nicht übertragen wurde. Ein Grund hierfür kann ein „Paketstau“ am Router sein, oder auf dem Zielrechner ist das IP-Protokoll nicht in der Lage, die Fragmente zu einem vollständigen Datenstrom zusammenzusetzen. Diese Meldung sollte man eingehend zulassen.

```
FORWARD -dir IN -prot ICMP_Typ_11 -src ANY:ANY -dest LOCAL_
CLIENT:ANY
```

## 2.1.20 Problemmeldungen

Typ 12 – Parameter-Problem: Dem Sender eines Datagramms teilt diese Meldung mit, warum das Datenpaket nicht übertragen wurde.

```
FORWARD -dir IN -prot ICMP_Typ_12 -src ANY:ANY -dest LOCAL_
CLIENT:ANY
```

Typ 4 – Source Quench: Die Puffer-Problem-Meldung teilt dem Sender des Datenpakets mit, warum das Datenpaket nicht übertragen wurde.

```
FORWARD -dir IN -prot ICMP_Typ_4 -src ANY:ANY -dest LOCAL_
CLIENT:ANY
```

## 2.1.21 Informationsmeldung

Typ 8 – Echo / Typ 0 – Echo Reply: An den Sender eines Echo Request werden vom Empfänger alle im Datenpaket enthaltenen Daten zurückgeschickt. Dadurch stellt man fest, ob eine bestimmte IP-Adresse erreichbar ist oder nicht. Viele selbst ernannte Hacker scannen das Internet mit Echo nach Rechnern, die mit Echo Reply antworten. Diese Rechner werden daraufhin auf Trojaner durchsucht. Daher sollte man Echo nur ausgehend und Echo Reply nur eingehend zulassen.

```
FORWARD -dir OUT -prot ICMP_Typ_8 -src ANY -dest ANY

FORWARD -dir IN -prot ICMP_Typ_0 -src ANY -dest ANY
```

## 2.1.22 File-Sharing-Tools: Gnutella

File-Sharing-Dienste wie Gnutella und eDonkey erfreuen sich steigender Beliebtheit. Sei es zum Tausch von Musikdateien, Videos oder erotischem Material zur Befriedigung unerfüllter Phantasien. So mancher Chef möchte seinen Mitarbeitern diese Dienste dennoch im Firmennetz zur Verfügung stellen, auch wenn sie nicht allzu viel mit der eigentlichen Arbeit zu tun haben. Auf den folgenden Seiten erläutern wir die hierzu nötigen Paketfilterregeln.

Gnutella: Der Peer-to-Peer-Dienst Gnutella ist einer der bekanntesten Tauschdienste. Um auf die File-Sharing-Dienste zugreifen zu können, müssen die TCP-Ports 6346 und 6347 ausgehend freigegeben werden.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
6346

FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
6347
```

## 2.1.23 File-Sharing-Tools: eDonkey und KaZaA

eDonkey: Standardmäßig nutzt eDonkey die Ports 4661, 4662 sowie 4665. Allerdings muss man zur Nutzung des Client nur den TCP-Port 4662 ausgehend öffnen. Der TCP-Port 4661 wird für den Serverbetrieb benötigt und ist somit für den Client nicht relevant. Die Nachrichtenfunktion von eDonkey nutzt den UDP-Port 4665.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
4662
```

Obiges Beispiel ist somit ausreichend. Will man einen Server laufen lassen und dazu noch Nachrichten mit anderen Usern austauschen, sind folgende Paketfilterregeln anzulegen.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
4661
FORWARD -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:
4662

FORWARD -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:
4665
```

KaZaA und Morpheus: Die beiden Peer-to-Peer-Tools KaZaA (www.kazaa.com) und Morpheus nutzen den TCP-Port 1214 zum Austausch von Daten mit anderen Anwendern.

```
FORWARD -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:
1214
```

## 2.1.24 Microsoft-Netzwerk

Microsoft Windows verwendet eine Reihe von Ports, um seine Netzwerkfunktionen zu erfüllen. In der alten Implementation, die bis Windows Me/NT zum Einsatz kam, waren das die Ports 137, 138 und 139. Seit Windows 2000 werden die Server Message Blocks über Port 445 versendet. Natürlich sind die Windows-Versionen ab 2000 auch rückwärts kompatibel, so dass beide Verfahren nebeneinander laufen können.

Über Port 137 wird der so genannte NetBIOS Name Service abgewickelt. Über diesen ordnet Windows – ähnlich wie bei DNS – Rechnernamen und IP-Adressen einander zu. Das führt unter Umständen zu folgendem Effekt: Surft ein Benutzer auf einem Windows-Webserver, kommt von diesem eine Anfrage auf Port 137 an den Rechner des Benutzers. Denn der Windows-Server nutzt die Winsock-Funktion gethostbyaddr(), um den Namen des entfernten Rechners aufzulösen. Unter Windows ist diese Funktion allerdings so implementiert, dass zunächst die NetBIOS-Namensauflösung versucht wird und erst bei einem Fehlschlag die DNS-Auflösung erfolgt.

Solcher Traffic sollte generell unterbunden werden, sowohl eingehend als auch ausgehend. Sollen zwei Windows-Netzwerke über das Internet Daten austauschen, ist generell ein VPN angeraten.

```
DROP -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:137

DROP -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:137

DROP -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:137

DROP -dir IN -prot TCP -src ANY:ANY -dest LOCAL_CLIENT:137
```

### 2.1.25 Microsoft Netzwerk Port 138

Hinter Port 138 versteckt sich der NetBIOS datagram service. Über diesen versendet Windows hauptsächlich Informationen über das Windows-Netzwerk, meistens per Broadcast. Beispielsweise der Windows-Dienst (**webcode: a944**) Computerbrowser nutzt NetBIOS-Nachrichten, um eine Liste aktueller Rechner im Windows-Netzwerk zu erstellen und über die Netzwerkumgebung anzuzeigen.

Die größte Gefahr bei den Datagram Services ist, dass ein Hacker Windows mittels gefälschter Pakete davon überzeugen kann, dass sein Rechner zum lokalen Netzwerk gehört und damit die Sicherheitsunterscheidung zwischen lokalen und Internet-Rechnern umgehen kann. Auch hier gilt, dass man diesen Port in beide Richtungen dicht machen sollte.

```
DROP -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:138

DROP -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:138

DROP -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:138

DROP -dir IN -prot TCP -src ANY:ANY -dest LOCAL_CLIENT:138
```

### 2.1.26 Microsoft Netzwerk Port 139

Der eigentliche Datenaustausch bei Windows-Netzwerken findet über Port 139 statt, den NetBIOS Session Service. Ist dieser Port offen, kann ein Hacker sich mit dem Rechner verbinden und versuchen, die Datei- und Druckerfreigabe zu hacken. Meist erfolgt das über eine Brute-Force-Attacke, bei der eine Vielzahl gängiger Passwörter ausprobiert wird.

Ein offener Port 139 verursacht zudem andere Probleme. So lauscht beispielsweise auch der Messenger-Dienst (**webcode: a944**) von Windows hier auf Nachrichten, die per net send geschickt werden. Häufig wird das zum Spammen missbraucht. Dabei kommt keine E-Mail beim User an, sondern ein Windows-Fenster mit dem Spam geht auf. Deshalb sollte dieser Port in beide Richtungen gesperrt werden.

```
DROP -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:139

DROP -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:139

DROP -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:139

DROP -dir IN -prot TCP -src ANY:ANY -dest LOCAL_CLIENT:139
```

## 2.1.27 Microsoft Netzwerk Port 135

Auch wenn Sie den Port 139 geschlossen haben, kann der Messenger-Spam bei Ihnen ankommen. Das Kommando net send nutzt ein undokumentiertes Feature des Microsoft RPC-Dienstes, der hinter Port 135 (epmap, endpoint mapper) auf eingehende RPC-Anfragen lauscht. Dieser bietet nämlich unter anderem eine Verbindung zum Messenger-Dienst, so dass net send diesen Weg als Alternative versucht, wenn der normale Zugang über Port 139 fehlschlägt. Inzwischen gibt es schon Spam-Tools, die gleich diese Methode nutzen, um den Spam abzusetzen.

Weitere Dienste, die ebenfalls über epmap versorgt werden, sind beispielsweise der DHCP-, der DNS- und der WINS-Server von Windows. Zudem wird Port 135 zur entfernten Administration für beinahe alle Windows-Dienste verwendet.

Dementsprechend gilt auch für diesen Port: sperren!

```
DROP -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:135

DROP -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:135

DROP -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:135

DROP -dir IN -prot TCP -src ANY:ANY -dest LOCAL_CLIENT:135
```

## 2.1.28 Microsoft Netzwerk Port 445

Mit Windows 2000 hat Microsoft das SMB-Protokoll um die Möglichkeit erweitert, komplett über TCP/IP abgewickelt zu werden – ohne den Umweg via „NetBIOS über TCP/IP“. Dazu verwendet Windows ausschließlich den Port 445 (microsoft-ds).

In einer Umgebung mit nur Windows 2000, XP und .NET Server 2003 können Sie diese Ports abschalten, indem Sie in den Optionen der Netzwerkkarte „NetBIOS über TCP/IP“ deaktivieren. Infolgedessen wird allerdings die Namensauflösung im LAN nur noch über DNS abgewickelt und nicht mehr über WINS oder NetBIOS-Broadcasts. Dann benötigen Sie also entweder einen DNS-Server im LAN,

der auch die lokalen Rechner verwaltet (etwa Windows 2000 als DHCP- und DNS-Server), oder Sie müssen auf jedem Rechner eine Host-Liste anlegen. Auch für den Port 445 gilt: SMB-Traffic hat nur innerhalb des LAN etwas zu suchen:

```
DROP -dir OUT -prot UDP -src LOCAL_CLIENT:ANY -dest ANY:445

DROP -dir IN -prot UDP -src ANY:ANY -dest LOCAL_CLIENT:445

DROP -dir OUT -prot TCP -src LOCAL_CLIENT:ANY -dest ANY:445

DROP -dir IN -prot TCP -src ANY:ANY -dest LOCAL_CLIENT:445
```

## 2.1.29 Microsoft Exchange

Der Exchange-Server von Microsoft agiert auf einer ganzen Reihe von Ports. Neben den bereits beschriebenen Ports für Mail- und News-Dienste – POP3, POP3S, SMTP, IMAP4 und IMAPS – kommen dazu noch X.400 MTA, LDAP, Secure LDAP und epmap. Letzterer dient zur entfernten Verwaltung des Exchange-Servers und sollte, wie bereits beschrieben, für den Zugriff von außen gesperrt werden. Da die Kommunikationsports auch von außen erreichbar sein sollen, müssen sie auf der Firewall für den Exchange-Server freigeschaltet werden, zumindest für SMTP, damit MTAs ihre Mails abliefern können:

```
FORWARD -dir IN -prot TCP -src ANY:ANY -dest EXCHANGE_SRV:25
```

Sollen die Postfachinhaber in der Lage sein, auch von extern auf ihre Mails zuzugreifen, sind die POP- und IMAP-Ports zu öffnen:

```
FORWARD -dir IN -prot TCP -src ANY:ANY -dest EXCHANGE_SRV:
110

FORWARD -dir IN -prot TCP -src ANY:ANY -dest EXCHANGE_SRV:
995

FORWARD -dir IN -prot TCP -src ANY:ANY -dest EXCHANGE_SRV:
143

FORWARD -dir IN -prot TCP -src ANY:ANY -dest EXCHANGE_SRV:
993
```

Über LDAP und Secure LDAP ermöglicht der Exchange-Server die Suche nach Namen, Telefonnummern und Mailadressen. Das sollte eigentlich den Benutzern im LAN vorbehalten sein:

```
DROP -dir IN -prot TCP -src ANY:ANY -dest ANY:389

DROP -dir IN -prot TCP -src ANY:ANY -dest ANY:636
```

Auf Port 102 wartet Exchange auf Anfragen von X.400-fähigen Mail Transfer Agents. Diesen können Sie je nach Bedarf freischalten.

### 2.1.30 Ports im Überblick

In der tecDaten-Tabelle (**webcode: d901**) haben wir für Sie alle wichtigen Ports zusammengestellt. Unsere Übersicht gibt Aufschluss darüber, welche Nebenstellen von welchen Applikationen verwendet werden und welches Protokoll zum Einsatz kommt: TCP oder UDP. Zudem haben wir jeweils die bekanntesten und häufigsten Trojaner und Würmer aufgeführt. Wir haben die Ports bewertet, so dass Sie in Zukunft genau wissen, welche Ports Sie bei der Konfiguration Ihrer Firewall freigeben oder sperren sollten.

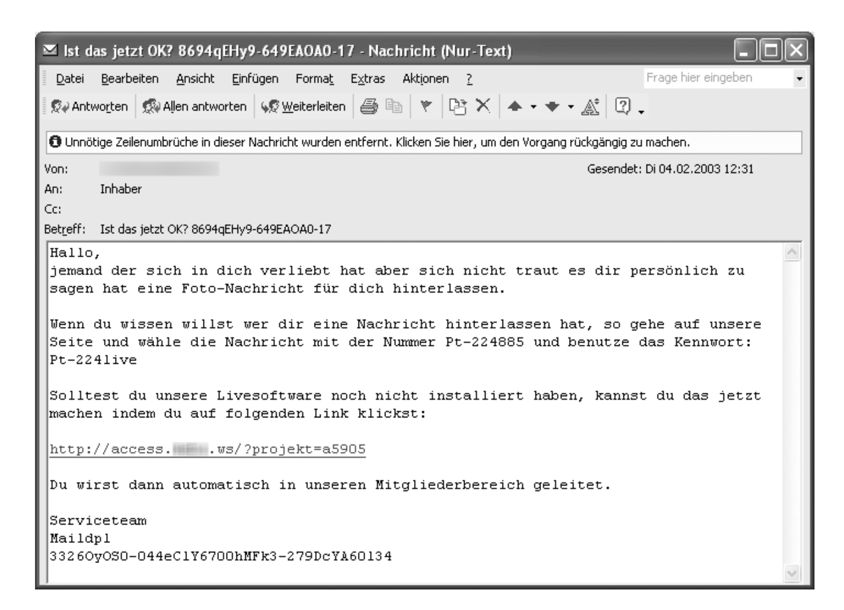
Konstantin Pfliegl, Mike Hartmann

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Grundlagen TCP/IP | a209 | – |
| Firewall-Grundlagen | a682 | – |
| So funktioniert E-Mail | a819 | – |
| Domain Name System | a205 | – |
| Sicher im Web unterwegs | a931 | – |

## 2.2 Spam-Schutz für Server

Im Laufe der Zeit sind Werbemails zu einem der größten Ärgernisse des Internets geworden. Zahlreiche Massenversender fluten Mailserver und Newsgroups mit ihren unerwünschten Nachrichten. Sowohl Benutzer als auch Systemadministratoren werden dadurch in zunehmendem Maße belästigt. Von diesen aggressiven Marketing-Maßnahmen kann jeder betroffen sein, der über eine eigene Mailadresse verfügt. Und tatsächlich blieb kaum jemand davon verschont.

Bereits im Januar 2001 rechnete die Studie „Unerbetene kommerzielle Kommunikation und Datenschutz" im Auftrag der Europäischen Union (www.europa.eu.int) mit rund 20 Milliarden Werbemails täglich. Eine interne Auswertung des Maildienstes GMX für den Zeitraum Mai bis Juli 2002 lieferte noch dramatischere Zahlen: Bei jeder siebten E-Mail von externen Servern handelte es sich um eine Spam-Mail, die von GMX abgewiesen wurde. So verhindern die Spam-Filter die Zustellung von 900 Spam-Mails pro Minute.




**Nicht nur aufdringlich:** Mail-Clients wie Outlook sind gefährdet, denn viele Spam-Versender wollen gleich den passenden Dialer einschmuggeln.

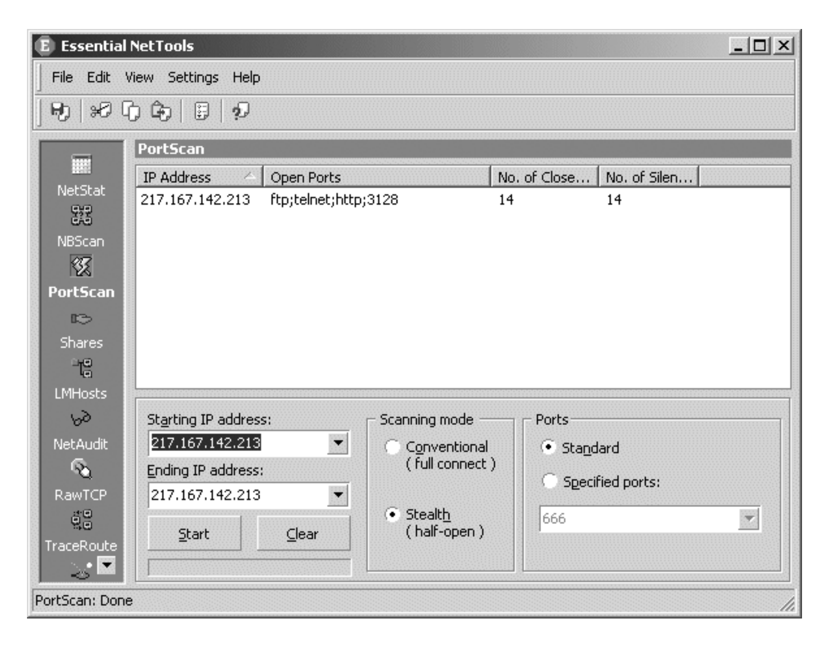
Das Schlimme an Spam ist nicht nur, dass es Zeit kostet, die Mails auszusortieren und zu löschen. Häufig verwenden die Spammer HTML- und Javascript-Code, um Dialer oder andere Bösartigkeiten auf den Rechner des Empfängers zu schleusen.

Um den zweifelhaften Marketing-Maßnahmen der Versender erfolgreich Einhalt zu gebieten, ist es erforderlich, das Versenden derartiger Massenmails schon im Vorfeld zu verhindern. Im folgenden Beitrag erläutern wir unter anderem, wie man verhindert, dass der eigene Mailserver für unautorisiertes Relaying verwendet wird und zeigen Möglichkeiten auf, Spam abzuwehren.

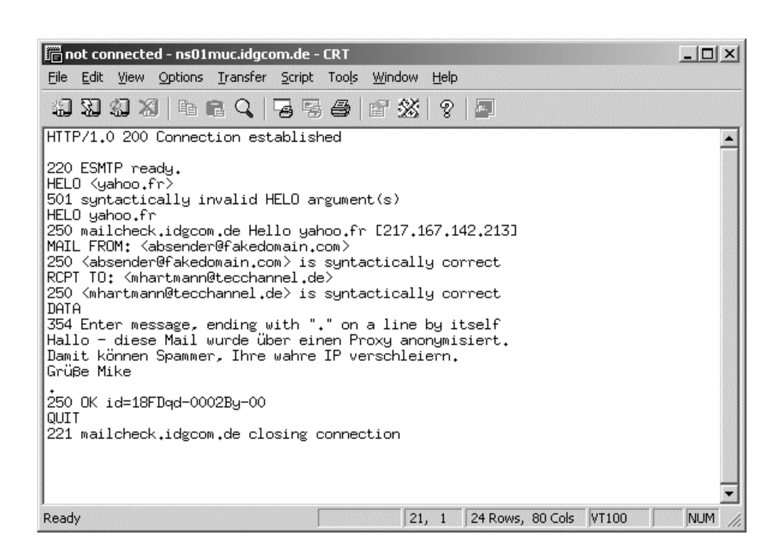
## 2.2.1 Wie arbeiten Spammer?

Ein Spammer hat kein Interesse daran, dass er sich in irgendeiner Form angreifbar macht. Also sucht er beim Versenden seiner Massenmails die Anonymität. Dazu hat er mehrere Möglichkeiten:

- Relaying – Dabei nutzt der Spammer einen ungenügend abgesicherten SMTP-Server, um unerkannt seinen Müll abzuladen.
- Smarthost – Dabei setzt der Spammer einen eigenen SMTP-Server ein, der die E-Mails ohne Umweg über einen weiteren Server direkt in die Empfänger-Mailbox pumpt.
- Proxy – Über einen offenen Proxy-Server kann der Spammer seine IP-Adresse zusätzlich verstecken, um einer Verfolgung zu entgehen.




**Kein Relay?** Doch, denn dieser Rechner hat einen offenen Proxy auf Port 3128, den der Spammer nutzen kann.




**Verschleiert:** Über einen offenen Proxy kann der Spammer seine IP-Adresse zusätzlich verschleiern.

Mit einer geeigneten Konfiguration der Mailserver-Struktur lässt sich eine ganze Menge Spam bereits im Vorfeld abfangen, so dass die eigenen Benutzer nicht davon betroffen werden. Der erste Schritt zu einem Spam-sicheren Mailserver ist jedoch eine Absicherung gegen den Missbrauch als offenes Relay.

## 2.2.2 Relaying – unerlaubtes Versenden von Mails

Spammer verwenden zum Versenden ihrer Massenmails grundsätzlich keine eigenen offiziellen Mailserver. Es ist gängige Praxis, zum Versenden fremde SMTP-Server zu missbrauchen. Man nennt dies Relaying. Die Gründe hierfür liegen auf der Hand: Anonymität und Kosten- sowie Zeitersparnis.

Der Spammer muss dazu nicht einmal besonders viel tun: Mittels spezieller Tools durchsucht er ganze IP-Adressbereiche nach Rechnern, bei denen Port 25 (SMTP) offen ist. Dort stellt er eine Verbindung her und versucht, eine Mail an einen Account bei einem Freemail-Anbieter zu senden – etwa relaytest@anbieter.com. Kommt diese Mail dort an, lässt sich der Server als Relay benutzen. Hat der Spammer genügend Relays gefunden, setzt er ein anderes Tool darauf an, so viele Mails wie möglich über die entsprechenden Server zu schicken, bevor diese eventuell dicht gemacht werden.

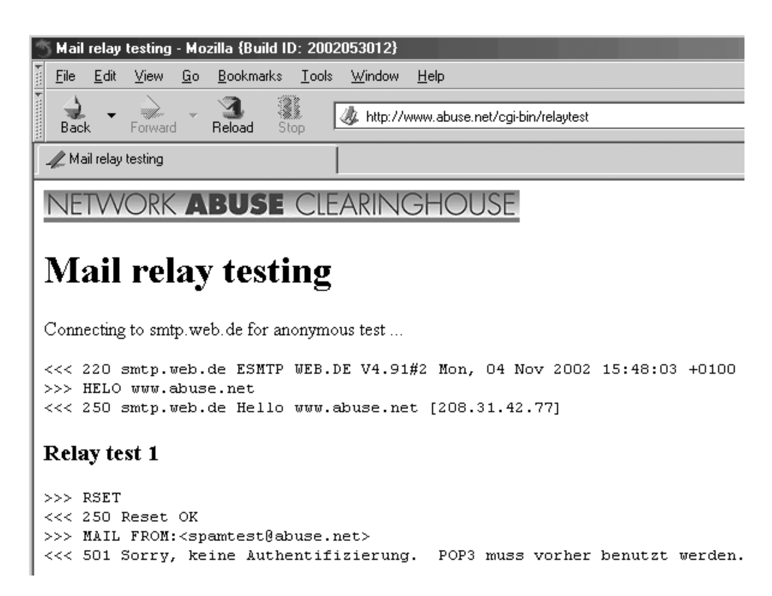
Wird ein Server häufig für unautorisiertes Relaying verwendet, landet er unter Umständen auf einer so genannten Blacklist. Andere SMTP-Server akzeptieren auf Grund dessen keine E-Mails mehr von diesem Server. Im schlimmsten Fall lassen

sich dann von diesem SMTP-Server gar keine Nachrichten mehr verschicken. Dabei ist Relaying nicht nur in vielen Ländern illegal, sondern bringt für den Betreiber des betroffenen Servers unter Umständen zahlreiche Probleme mit sich:

- Er bleibt auf den Kosten für das entstehende Datenvolumen sitzen.
- Das massive Mailaufkommen behindert seine Infrastruktur.
- Er wird mit Sicherheit eine Vielzahl von Mails verärgerter Spam-Empfänger bekommen.
- Unter Umständen landet er auf einer schwarzen Liste, so dass die Mails seiner Anwender bei manchen Mailservern nicht mehr angenommen werden.

## 2.2.3 Relaying möglich?

Wenn Sie einen eigenen SMTP-Server an das Internet angeschlossen haben, sollten Sie diesen auf Relaying überprüfen und gegebenenfalls davor schützen. Um zu testen, ob Ihr Server gegen Missbrauch durch Relaying gesichert ist, haben Sie mehrere Möglichkeiten. Auf den Webseiten von abuse.net (www.abuse.net) finden Sie einen Mail-Relay-Test. Dieser Schnelltest liefert Ihnen einen ersten Überblick über Ihren Server, indem er eine Reihe bekannter Relay-Tricks an Ihrem Server ausprobiert und Ihnen die Ergebnisse der Tests übersichtlich aufzeigt.




**Gesperrt:** Der SMTP-Server von web.de lässt uns nur Mails verschicken, wenn wir uns zuvor mit POP3 angemeldet haben.

Eine andere Möglichkeit zum Test bietet die Open Relay Database ordb.org (www.ordb.org). Durch die Nutzung dieser Datenbank unterbinden Systemadministratoren den E-Mail-Austausch mit offenen Relay-Servern. Hierzu verwaltet ordb.org eine Liste von Hosts beziehungsweise IP-Adressen, welche nachweislich als offene SMTP-Relays arbeiten. Jeder kann seinen Mailserver auf den Seiten der Organisation zum Test anmelden. Die Sache hat allerdings einen Haken: Ist das Ergebnis des Tests positiv, da Ihr Server E-Mails als Relay weitergeleitet hat, wird Ihr SMTP-Server auch gleich in der Open Relay Database gelistet. Einige Systeme werden nun unter Umständen von Ihnen keine Mails mehr akzeptieren.

Details über die Open Relay Database finden Sie unter der Internet-Adresse www.ordb.org/faq/. Dort gibt es auch mehrere Anleitungen, wie man sie mit diversen Mailservern, beispielsweise Sendmail, einsetzt.

## 2.2.4 Relaying möglich – was nun?

Da es unerlässlich ist, dass ein SMTP-Server unautorisiertes Relaying erkennt und ablehnt, gibt es in einer SMTP-Sitzung vier Elemente zur Identifizierung von Sender und Empfänger mit unterschiedlichem Sicherheitsgrad:

| Identifizierung von Sender und Empfänger bei einer SMTP-Sitzung | |
|---|---|
| **Element** | **Beschreibung** |
| HELO Hostname | Es kann keiner oder jeder beliebige Hostname angegeben werden. |
| MAIL From: | Der Client kann jede beliebige Adresse angeben. |
| RCPT To: | Dies muss eine korrekte Adresse sein. |
| SMTP_CALLER | IP-Adresse des Client. |

Die ersten beiden Punkte (HELO und MAIL) können beliebige Angaben enthalten und tun dies auch oft. Auf diese Angaben sollte man sich also nicht verlassen. Stattdessen sollte der Mailserver das Relaying an Hand der folgenden Kombination zulassen: „RCPT To: Adresse (Domain-Name)“, „SMTP_CALLER Domainname“ sowie „SMTP_CALLER IP-Adresse“. Dabei empfiehlt es sich, folgenden Algorithmus anzuwenden.

- Handelt es sich bei „RCPT To“ um eine der „eigenen“ Domains, ist „RCPT To“ lokal oder akzeptiert der eigene Mailserver das Weiterleiten von Mails an diese Domain (MX Record), ist die Weiterleitung erlaubt.
- Ist der unter „SMTP_CALLER“ angegebene Domain-Name bekannt und autorisiert, beziehungsweise die IP-Adresse, wird Relaying akzeptiert.
- In allen anderen Fällen wird das Relaying unterbunden.

Zudem sollte der SMTP-Server einen etwaigen unter „MAIL From:“ angegebenen Domain-Name auf dessen Richtigkeit überprüfen. Liefert eine DNS-Abfrage kein Ergebnis, existiert der Domain-Name nicht. So sollte das Relaying unabhängig von den anderen Faktoren verhindert werden.

### 2.2.5 Weitere Maßnahmen gegen Relaying

Eine weitere sichere Möglichkeit gegen unautorisiertes Relaying ist die SMTP-Authentifizierung, smtp-auth genannt. Der Mailserver erlaubt nur den Clients, die sich mit einer gültigen Kombination aus Benutzername und Kennwort identifizieren, eine Weiterleitung. Das Verfahren entspricht dem Quasi-Standard RFC 2554, der von gängigsten Mail-Clients unterstützt wird.

Einige Provider setzen die SMTP-Authentifizierung nicht ein, da dies nicht von jedem System unterstützt wird. Stattdessen wird das Relaying dynamisch freigeschaltet. Der Client ruft seine neuen Nachrichten wie bisher über POP3 oder IMAP4 vom Server ab. Dabei identifiziert sich der Client gegenüber dem Server mit Benutzername und Passwort und übermittelt auch seine IP-Adresse. Der Mailserver erlaubt nun dieser IP-Adresse den Versand von E-Mails für eine bestimmte Zeit, in der Regel zehn bis fünfzehn Minuten. Bei „SMTP after POP“ muss somit zumindest einmal vor dem Senden einer Mail das entsprechende POP3-Postfach abgefragt worden sein.

Allerdings benötigen Sie dann zwei SMTP-Server – einen ohne „SMTP after POP“, der nur für eingehende Mails zuständig ist, und einen zweiten, den die eigenen Benutzer für ausgehende Mails nutzen können. Ersterer muss im DNS als Mail-Exchanger (MX) ausgewiesen sein.

### 2.2.6 Relaying und Sendmail

Seit der Version 8.9 ist das Relaying in Sendmail per Default deaktiviert. Der Mailserver nimmt von außen keine E-Mails zur Weiterleitung an, es sei denn, sie betreffen die eigene Domain. In früheren Sendmail-Versionen ist das Relaying standardmäßig aktiviert. Ist bei Ihnen noch eine ältere Version des SMTP-Servers im Einsatz, sollten Sie das Relaying so schnell wie möglich deaktivieren.

Für ein kontrolliertes Relaying ist es die einfachste Lösung, alle Domains, für welche Relaying möglich sein soll, in der Datei /etc/mail/relay-domains einzutragen. Für alle Einträge in dieser Datei ist das Relaying gestattet. Eine detaillierte Anleitung zur Anti-Spam-Konfiguration finden Sie auf den Webseiten des Sendmail-Projekts (www.sendmail.org).

Falls bei Ihnen Microsofts Exchange 2000 Server im Einsatz ist, finden Sie unter der Internet-Adresse www.msexchangefaq.de einen Workshop zur Konfiguration von Relaying.

### 2.2.7 Heikle SMTP-Kommandos

Die beiden SMTP-Kommandos VRFY und EXPN bieten Spammern die Möglichkeit zu überprüfen, ob eine E-Mail-Adresse gültig ist (VRFY) und liefern auch gleich noch mehr Adressen (EXPN). Daher sollten Systemadministratoren festlegen, wer diese beiden Kommandos nutzen darf und wer nicht.

Mit dem VRFY-Kommando übergibt der Client dem Server eine Mailadresse, der Server antwortet daraufhin mit der Information, ob die entsprechende Adresse auf dem System existiert oder nicht. Dieses Kommando ist jedoch nach RFC 821 erforderlich. Daher sollte man den Mailserver dahingehend konfigurieren, dass er das Kommando wie im SMTP-Standard vorgesehen zur Verfügung stellt, als Antwort jedoch stets „252 Argument not checked“ zurückliefert.

Die meisten Mailserver, wie beispielsweise Sendmail, behandeln das Kommando EXPN wie VRFY. Ist dies bei der von Ihnen eingesetzten Server-Software nicht der Fall, sollten Sie das Kommando EXPN deaktivieren, sofern dies möglich ist. Mit diesem Kommando kann ein Client Mailing-Listen überprüfen und sich vom Server sämtliche Mitgliederadressen ausgeben lassen.

### 2.2.8 Blackhole Lists und andere Maßnahmen

Beim Kampf um Spam gilt es nicht nur, den eigenen Mailserver vor unautorisiertem Relaying zu schützen, sondern auch eingehende Spam-Mails zu erkennen und gegebenenfalls abzuweisen. In diesem Fall kommen die so genannten Realtime Blackhole Lists (RBLs) zum Einsatz. Diese werden von unabhängigen Institutionen betrieben und lassen sich meist gratis nutzen. Die Bedienung ist einfach: Der eigene Mailserver schickt eine DNS-Anfrage mit der IP-Adresse an die Datenbank. Kommt ein Ergebnis zurück, handelt es sich hierbei um einen bekannten Spammer. Ein anderer Typ von RBLs listet nicht bekannte Spam-Quellen, sondern offene Mail-Relays. Ein Beispiel hierfür ist die schon erwähnte ORDB-Datenbank.

### 2.2.9 Teergruben

Wer im Kampf gegen Spammer einen Schritt weiter gehen will, kann vor seinen Mailserver eine so genannte Teergrube schalten, die den Spammer ausbremst. Die Arbeitsweise von Teergruben ist einfach: Ein Rechner kann theoretisch maximal rund 65.000 TCP/IP-Verbindungen gleichzeitig offen halten, in der Praxis sind dies allerdings weniger. Wenn es nun gelingt, einen Port bei der Mailauslieferung unnötig lange offen zu halten, so reduziert sich die Leistungsfähigkeit des Rechners des Spammers – also die Anzahl der pro Stunde ausgelieferten Mails.

Hierbei kommen die Fortsetzungszeilen des SMTP-Protokolls zum Einsatz (NOOP). Diese bieten die Möglichkeit, eine SMTP-Session über lange Zeit offen zu halten, ohne dass es zu einem TCP-Timeout und somit zu einem Abbruch der

Session kommt. Außer dem erzieherischen Wert haben diese Teergruben jedoch keine weiteren Vorteile. Fertige Teergruben finden Sie zum Beispiel auf den Internet-Seiten von abuse.net (spam.abuse.net).

## 2.2.10 Anbieter rüsten auf

Auch die großen Maildienste und Webhoster haben die Spam-Problematik erkannt und ergreifen Gegenmaßnahmen. Der E-Mail-Dienst GMX (www.gmx.de) betreibt kein offenes SMTP-Relay. Für den Versand von Nachrichten muss der Sender über eine bei GMX registrierte Absenderadresse verfügen. Zudem akzeptiert der Mailserver grundsätzlich nur E-Mails für die eigenen gehosteten Adressen (gmx.de, gmx.net etc.).

GMX überprüft die Mails nicht automatisch auf Inhalte, um zu entscheiden, ob es sich um Spam handelt. Nutzer des Dienstes haben die Möglichkeit, unerwünscht erhaltene Werbemails komplett und mit vollständigem Mail-Header zur Auswertung an abuse@gmx.net zu schicken. GMX verwaltet eine interne Liste von E-Mail-Adressen, die für den Versand von E-Mail-Werbung an Personen bekannt sind, die dem Empfang dieser Werbung nicht ausdrücklich zugestimmt haben. Zum Schutz vor Mailbomben lehnt GMX Mails vom gleichen Absender automatisch ab, sofern ein fest definiertes Limit eingehender Mails in einem bestimmten Zeitraum überschritten wird.

Der Webhosting-Anbieter 1&1 Puretec startete im Juli 2002 eine Anti-Spam-Initiative für die über zwei Millionen gehosteten Postfächer. Ein Maßnahmenbündel, bestehend aus dem Einsatz neuer Mailserver mit SMTP-auth sowie speziellen Filtertechnologien, soll den meisten Spam verhindern.

Der von 1&1 entwickelte Spam-Filter weist nach Angaben des Unternehmens pro Tag rund 300.000 Nachrichten von unsicheren Mailservern und Proxies zurück. Die Kunden des Unternehmens sollten für einen uneingeschränkten Nachrichtenversand auf die neuen Mailserver mit SMTP-Authentifizierung umstellen. Ein Spam-Blocker limitiert die über die alten Server eingelieferten Mails pro Benutzer und Stunde.

Konstantin Pfliegl

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| So funktioniert E-Mail | a819 | – |
| So funktioniert TCP/IP | a209 | – |
| DNS: Domain Name System | a205 | – |
| Kampf gegen Spam | a323 | – |

## 2.3 Sicherheit im WLAN

Selbst Laien können mit einfachen Tools in Funknetze eindringen. Speziell wenn es um sensible Daten geht, muss man Vorkehrungen treffen, die das Abhören und unerlaubte Nutzen des WLANs erschweren.

Drahtlose lokale Netze (Wireless LAN – WLAN) erfreuen sich steigender Beliebtheit und Verbreitung. Vor allem der IEEE 802.11b-Standard setzt sich zunehmend durch. Neben der Planung, Installation und Administration ist dem Sicherheitsaspekt bei WLANs besondere Aufmerksamkeit zu schenken. Außer der grundlegenden Problematik der offenen Ausbreitung der Funkwellen kommt erschwerend hinzu, dass Teile der Funknetzstandards prinzipbedingt nicht sicher sind.

Dieser Artikel beschreibt zunächst die Sicherheitslücken, insbesondere des aktuell boomenden IEEE 802.11-Standards. Anschließend zeigt er Wege, um sich gegen Angriffe zu schützen und gibt einen Ausblick auf die zukünftigen technischen und standardbezogenen Entwicklungen.

### 2.3.1 Mangelhafte Sicherheit mangelhaft genutzt

Die Sicherheitsproblematik ist bei allen drahtlosen Systemen besonders relevant. Auf Grund der Ausbreitungscharakteristik elektromagnetischer Wellen ist ein Abhören oder Senden auf der physikalischen Ebene möglich, ohne dass beispielsweise in das Gebäude eingedrungen werden muss (Parking Lot Attack). Hierin besteht ein wesentlicher Unterschied zu drahtgebundenen Übertragungsprotokollen. Bei diesen kann im Normalfall außerhalb des Firmengebäudes nur der für extern bestimmte Datenverkehr beobachtet werden.

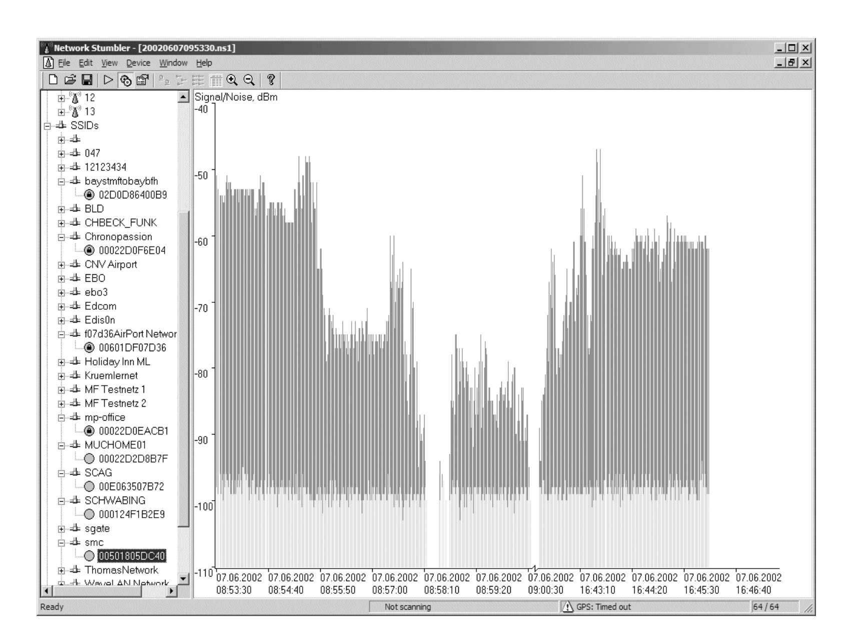
Erschwerend kommt hinzu, dass WLAN-Systeme ein komfortables Ad-hoc-Networking ermöglichen sollen. Die Identifizierung, Authentifizierung und Anmeldung (Autorisierung) der Stationen muss dabei möglichst automatisch ablaufen. Die am Markt verfügbaren WLAN-Systeme sehen in der Regel zwar Sicherheitsmechanismen vor, doch haben diese zum Teil erhebliche Lücken. Dadurch sind Angriffe relativ leicht möglich. Dabei unterscheidet man zwischen passiven (Abhören) und aktiven Angriffen (Eindringen).

Von den Sicherheitslücken sind besonders die Systeme nach IEEE 802.11 betroffen. Deswegen führen wir die weitere Diskussion an diesem Beispiel. Bei den anderen Systemen sind vergleichbare Risiken noch nicht öffentlich bekannt.

### 2.3.2 Kostenlose Werkzeuge für den Angriff

Angriffe auf WLANs sind mit herkömmlichen Geräten aus der Serienproduktion und selbst mit preiswerten WLAN-Karten möglich. Passende Software-Werkzeuge gibt es kostenlos und öffentlich im Internet. Sie messen Funkfelder sehr ein-

fach aus und ermitteln grundlegende Informationen über nicht geschützte Netze. Die Windows-Anwendung Network Stumbler kann man beispielsweise unter der Adresse www.netstumbler.com herunterladen.




**Gescannt:** NetStumbler liefert viele Informationen aller gefundenen Funknetze.

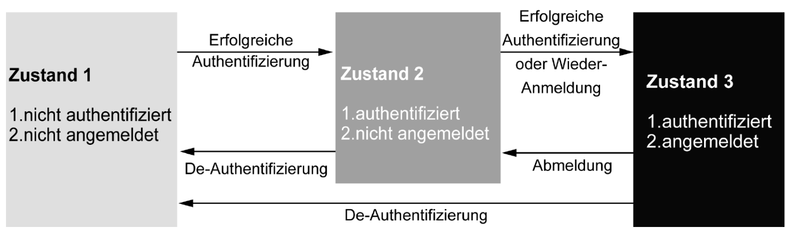
Mittlerweile stehen verschiedene Erweiterungen zur Verfügung, die einen sicheren Betrieb ermöglichen sollen. Diese Ansätze sind aber bislang herstellerspezifisch, da zum gegenwärtigen Zeitpunkt kein umfassender Standard existiert.

Ungeachtet der bekannten Risiken werden in der Praxis selbst die zur Verfügung stehenden Mechanismen nur unzureichend genutzt. Dies macht Angriffe selbst für Laien ohne Weiteres möglich. Als populäres Beispiel sehen Sie unter www.sfdrs.ch/content/news/10vor10/archiv_sendung.php?docid=20010524 eine Reportage des Schweizer Fernsehens.

## 2.3.3 Sicherheitsarchitektur und Authentifizierung

Der IEEE802.11-Standard sieht im Rahmen seiner Sicherheitsarchitektur drei verschiedene Zustände vor, um zwischen assoziierten und authentifizierten Stationen zu unterscheiden. Authentifizierung und Anmeldung bilden zusammen ein zweistufiges Zuordnungssystem:

- Eine Station kann sich nur anmelden, wenn sie authentifiziert ist. Dabei versteht man unter Authentifizierung den Nachweis, dass eine Station auch diejenige ist, die sie vorgibt zu sein.
- Eine Station kann das Verteilungssystem nur dann nutzen, wenn sie bei einer Zelle angemeldet ist.




**Dreistufig:** Die Sicherheitsarchitektur des 802.11-Standards sieht drei Zustände vor, um zwischen assoziierten und authentifizierten Stationen zu unterscheiden.

Im Rahmen der Authentifizierung wird die Identität von Stationen überprüft. Dabei stehen zwei Methoden zur Authentifizierung zur Verfügung:

- Die offene Authentifizierung (Open Authentication) folgt einem sehr einfachen Algorithmus, der die Funktion einer Authentifizierung nur formal erfüllt.
- Die Authentifizierung durch gemeinsame Schlüssel (Shared Key Authentication) beruht auf der Überprüfung, ob die beiden beteiligten Stationen denselben geheimen Schlüssel aufweisen. Er basiert auf dem WEP-Algorithmus und weist somit dessen Sicherheitslücken auf.

## 2.3.4 Zugangskontrolle

Auf der niedrigsten Ebene erfolgt die Zulassung der Teilnehmer anhand eines Schlüssels, der als Electronic Service Set ID (SSID, ESSID) bezeichnet wird. Diese ID wird von einem Administrator in allen mobilen Teilnehmern und allen Zugangspunkten eingetragen. Dieser zeigt die Zugangsrechte des Client an, aber nicht die eindeutige Identifikation. Dabei ergeben sich zwei Einschränkungen:

- Es ist häufig kein Problem, eine allgemeine Zugangsnummer herauszufinden, um den Verkehr auf dem Netzwerk unberechtigt abzuhören.
- Darüber hinaus erlauben die meisten Hersteller von mobilen Stationen die Angabe der Option „any“ in ihren Konfigurationsdateien, wodurch der Einsatz in allen Netzwerken authentisiert ist.

Weiterhin können die MAC-Adressen der mobilen Teilnehmer in die Zugangslisten (ACL) der Access Points eingetragen werden. Auch hier sind zwei Einschränkungen zu verzeichnen:

- Die MAC-Adresse des mobilen Teilnehmers lässt sich bei den meisten auf dem Markt verfügbaren Produkten verändern, so dass ein Missbrauch möglich ist.
- Im Bereich kleiner drahtloser Netzwerke sind ACLs recht problemlos umzusetzen. Bei großen Netzwerken mit mehreren Zugangspunkten erfordert dies jedoch eine umfangreiche Administration jeder Station. Nur so ist für jeden Teilnehmer ein Wechsel zwischen den Funkzellen möglich (Roaming). Bislang bieten nur einige wenige Hersteller komfortable Werkzeuge zur Verwaltung größerer drahtloser Netzwerke an.

### 2.3.5 Mehr Sicherheit mit WEP

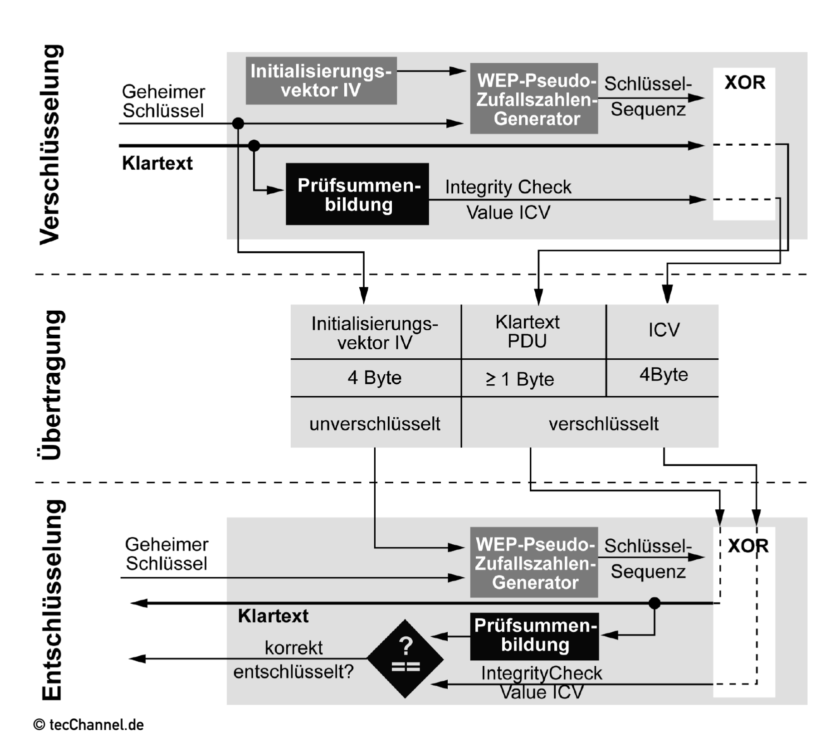
WEP stellt einen optionalen Bestandteil des IEEE802.11-Standards dar. Um ein 802.11-konformes System anzubieten, muss WEP also nicht zwingend implementiert sein. Die im Standard vorgesehene Variante von WEP sieht eine Kodierung mit einem 40 Bit langen Schlüssel vor. Darüber hinaus bieten einige Hersteller eine Kodierung mit 128 Bit an. Hierbei handelt es sich unter Umständen um proprietäre Entwicklungen, die die Interoperabilität der Systeme unterschiedlicher Hersteller behindern.

Die Verschlüsselung im Rahmen des IEEE802.11 wird nicht nur für die Verschlüsselung der zu übertragenden Informationen eingesetzt, sondern auch für die Authentifizierung von Stationen. Die Kenntnis des Schlüssels ermöglicht also nicht nur das Abhören der versendeten Pakete, sondern auch das Eindringen in das entsprechende Netzwerk.

Der Generator basiert auf dem RC4-Verschlüsselungsalgorithmus (Key Scheduling Algorithm – KSA), der mit einem statischen WEP-Schlüssel von 40 Bit oder 128 Bit (WEP2) arbeitet. Dabei wird im Rahmen eines so genannten Stromverschlüsselers (Stream Encryption) für jedes Datenpaket ein neuer Schlüssel generiert. Dies ist von zentraler Bedeutung, damit gleiche Klartextpakete nicht zu gleichen Schlüsseltextpaketen führen.

### 2.3.6 Unendlich langer Pseudo-Schlüssel

Für die Verschlüsselung wird auf der Grundlage eines vergleichsweise kurzen Schlüssels und eines zufällig bestimmten Initialisierungsvektors (IV) mit Hilfe eines Generators für Pseudo-Zufallszahlen eine unendlich lange Schlüsselfolge generiert. Mit dieser erfolgt die bitweise Verknüpfung des Klartextes mit einem Exklusiv-Oder-Gatter. Das Verfahren verschlüsselt Klartext als auch die Prüfsumme und überträgt diese mit dem unverschlüsselten Initialisierungsvektor.




**WEP:** Verschlüsselung, Übertragung und Entschlüsselung nach dem Wired-Equivalent-Privacy-Algorithmus.

Auf der Empfängerseite wird der verschlüsselte Text mit dem ebenfalls expandierten Schlüssel mit einer Exklusiv-Oder-Verknüpfung entschlüsselt. Das WEP-Verfahren basiert also auf einem symmetrischen Algorithmus, bei dem Sender und Empfänger einen gemeinsamen Schlüssel (Shared Key) verwenden.

Der Vorteil des Verfahrens besteht darin, dass es jedes Paket mit einer anderen Zeichenfolge verschlüsselt. Rückschlüsse auf die übertragenen Zeichen durch Ausnutzen von statistischen Verteilungen werden auf diese Weise erschwert.

## 2.3.7 WEP-Sicherheitsrisiken

Die Verwendung eines statischen Schlüssels ist zwar vergleichsweise einfach zu realisieren, birgt aber ein signifikantes Sicherheitsrisiko, da nach dessen Bekanntwerden kein Schutz mehr gegeben ist. Dabei sind zwei grundsätzliche Möglichkeiten zu unterscheiden, um an einen statischen Schlüssel zu gelangen:

Erstens kann der Schlüssel über den menschlichen Weg bekannt werden. Dies ist insbesondere dann kritisch, wenn in einem Unternehmen alle Stationen den identischen statischen Schlüssel besitzen. Allerdings ist das Auslesen an den mobilen Stationen meist nicht unmittelbar möglich, da der Schlüssel auf der Karte in einem geschützten Flash -Speicher abgelegt ist.

Zweitens kann ein Angreifer durch verschiedene Algorithmen versuchen, den Schlüssel zu rekonstruieren. Hier sind folgende Ansätze zu beobachten:

- Die Verschlüsselung eines Pakets erfolgt ausgehend von einem Initialisierungsvektor (IV). Dieser 24 Bit lange IV wird anhand eines feststehenden Algorithmus mit jedem neuen Paket verändert. Dies bedeutet, dass nach $2^{24}$, rund 16,7 Millionen Paketen, wieder mit der gleichen Abfolge von Initialisierungsvektoren begonnen wird. Entsprechend liegen dann der Verschlüsselung der folgenden Pakete die gleichen Zeichenfolgen zu Grunde.
- Im Rahmen der so genannten Known-Plain-Text-Angriffe werden Rückschlüsse auf den verwendeten Schlüssel über Paare von bekannten und verschlüsselten Daten gezogen. Bekannte Daten kann ein Angreifer zum Beispiel aus der Struktur von IP-Paketen ableiten.
- Darüber hinaus ist die Kombination einer Stromverschlüsselung, wie sie durch RC4 vorgegeben ist, mit einer Fehlererkennung durch einen linearen Cyclic Redundancy Check (CRC) unsicher. Zum einen treten nachvollziehbare Abhängigkeiten zwischen den zu übertragenden Daten auf. Zum anderen können Modifikationen in den Paketen unentdeckt bleiben, wenn die CRC-Daten entsprechend angepasst werden.

Insbesondere auf der Schwäche der Initialisierungsvektoren basieren Werkzeuge wie Airsnort (http://airsnort.sourceforge.net) und Wepcrack (http://sourceforge.net/projects/wepcrack), die kostenlos und frei über das Internet verfügbar sind. Mit diesen finden Hacker die verwendeten Schlüssel innerhalb weniger Stunden heraus. Sowohl die hierfür benötigte kriminelle Energie als auch die erforderlichen Kenntnisse, Werkzeuge und Fähigkeiten sind vergleichsweise gering. Dabei ist zu vermerken, dass auf Grund dieser Schwäche die Sicherheit der Verschlüsselung nicht exponentiell zunimmt, wie dies bei der Verwendung eines linearen Schlüssels der Fall wäre. Die Komplexität steigt bestenfalls linear.

### 2.3.8 Gegenmaßnahmen

Folgende Anforderungen muss ein sicheres WLAN in der Praxis erfüllen:

- Umfassende Authentifizierung: In einer umfassenden Sicherheitsarchitektur müssen alle an einem Netzwerk beteiligten Stationen ihre Identität nachweisen (Mutual Authentication). Dies ist eine Anforderung, die vor allem von drahtlosen oder mobilen Stationen gestellt wird. Denn nur durch eine wechselseitige Authentifizierung kann sichergestellt werden, dass sich ein mobiler Teilnehmer keinem „feindlichen“ Netzwerk anvertraut. In einer bekannten und fest

verdrahteten Umgebung ist das Risiko, an einen feindlichen Partner zu gelangen, unvergleichlich geringer, da hierfür die bestehende Netzwerkinfrastruktur bereits modifiziert worden sein muss.

- Flexibilität: Die Sicherheitskonzepte müssen die Anforderungen unterschiedlicher Nutzergruppen erfüllen. So gilt es etwa in einem Firmennetz, die User zu beschränken, während ein Service Provider für alle Nutzer offen ist, aber dennoch den Verkehr unterschiedlicher Nutzer getrennt „sichern“ muss.
- Mobilität: Sie muss im Rahmen eines Roaming unterstützt werden. Hierdurch kommt praktisch nur eine zentralisierte Serverrealisierung in Frage.
- Vertraulichkeit: Sie erfordert ein Konzept, das nicht nur auf einer Information, wie einem statischen Schlüssel, basiert. Ein solcher Schlüssel kann über den menschlichen Weg oder beim Diebstahl einer mobilen Station bekannt oder durch Lauschangriffe herausgefunden werden. Eine dynamische Schlüsselverwaltung erscheint unumgänglich. Auch muss die Verwaltung und Verteilung der Schlüssel selbst sicher sein. Bei der Verteilung der Schlüssel darf man keine Rückschlüsse auf die verwendeten Schlüssel ziehen können.
- Skalierbarkeit: Die Systeme müssen skalieren. Dies bedeutet, dass auch der Einsatz mehrerer hundert oder tausend Stationen möglich sein muss. Diese für das allgemeine Unternehmensumfeld sicherlich sinnvolle Anforderung führt aber leider bei einer Reihe der vorgestellten Lösungen zu einem hohen Aufwand, der in kleineren SOHO-Netzen in der Regel nicht zu leisten ist.

### 2.3.9 Aufwendigere Verschlüsselung

Der Einsatz einer stärkeren Verschlüsselung verringert zwar die Gefahr, dass durch Abhören Rückschlüsse auf den verwendeten Schlüssel gezogen werden können, da der Rechenaufwand für das Herausfinden des Schlüssels steigt. Das grundsätzliche Risiko eines statischen und symmetrischen Schlüssels bleibt aber bestehen, ebenso wie die Gefahr des Eindringens in das Netzwerk.

Da die beschriebenen Mängel auch beim IEEE bekannt sind, wurde dort die Task Group i (http://grouper.ieee.org) (TGi) ins Leben gerufen. Sie soll einen Nachfolger für WEP entwickeln und standardisieren. Nach verschiedenen Ansätzen ist gegenwärtig jedoch leider keine große Bereitschaft dieser Task Force wahrzunehmen, einen einheitlichen Standard auf den Weg zu bringen. Verschiedene konkurrierende herstellerspezifische Lösungen sind jedoch schon auf dem Markt verfügbar. Auf diese sind die Anwender gegenwärtig angewiesen. Hier zwei typische Beispiele, die andere Hersteller in ähnlicher Art verfolgen.

Lucent bietet mit WEPplus eine WEP-Erweiterung an, die speziell die Angreifbarkeit durch AirSnort eliminieren soll. Hierzu wird ein anderer Algorithmus für die Erzeugung der Initialisierungsvektoren (IV) eingesetzt. Diese Lösung erfordert lediglich ein Treiber-Update. Da der IV von der sendenden Station vorgegeben und im Datenpaket mit übertragen wird, ist WEPplus abwärts kompatibel.

Die Firma RSA Data Security (www.rsasecurity.com), die den RC4-Algorithmus erfunden hat, bietet mit der als Fast Packet Keying (FPK) bezeichneten Erweiterung ebenfalls eine Lösung. FPK erzeugt aus dem konstanten, vorgegebenen Schlüssel sowie der ebenfalls konstanten Senderadresse und einem paketspezifischen IV mittels eines Hashing-Algorithmus für jedes Datenpaket einen individuellen 104 Bit langen Paketschlüssel. Auf diese Weise wiederholen sich die IV erst nach $2^{103}$, statt wie bisher nach $2^{24}$ Paketen.

## 2.3.10 Authentifizierung via EAP und 802.1X

Das Extensible Authentication Protocol (EAP – RFC 2284) stellt ein grundlegendes Fundament für eine umfassende und zentralisierte Sicherheitskonzeption dar. Es wurde ursprünglich für PPP-Links entwickelt, um eine zuverlässige Authentifizierung von Remote-Access-Usern bereitzustellen. EAP ist ein allgemeines Protokoll, das mehrere Authentifizierungsmöglichkeiten bietet. Die Auswahl des Verfahrens findet im Point-to-Point Protocol erst nach der Link Control Phase (LCP) in der Authentifizierungsphase statt.

| Rahmenformat der in Ethernet gepackten EAP-Pakete | | |
|---|---|---|
| **Byte** | **Beschreibung** | **Anmerkung** |
| 1-7 | Preamble | |
| 8 | Start Delimiter | |
| 9-14 | Destination Address | |
| 15-20 | Source Address | |
| 21-22 | Length / Type | Port Access Entity (PAE) Ethernet Type |
| 23 | Protocol Version | 0000 0001 als Standard |
| 24 | Packet Type | 0000 0000 EAP-Packet<br>0000 0001 EAPOL-Start<br>0000 0010 EAPOL-Logoff<br>0000 0011 EAPOL-Key<br>0000 0100 EAPOL-Encapsulation-ASF-Alert |
| 25-26 | Packet Body Length | vorhanden nur für EAP-Packet, EAPOL-Key, EAPOL-Encapsulation-ASF-Alert |
| 27-N | Packet Body | vorhanden nur für EAP-Packet, EAPOL-Key, EAPOL-Encapsulation-ASF-Alert |

**Im Rahmen:** Das Rahmenformat der in Ethernet eingepackten EAP-Pakete.

Von PPP ausgehend hat EAP mittlerweile auch Zugang in den im Jahr 2001 verabschiedeten IEEE802.1X gefunden, der die physische Übertragung auf LAN-Netzwerke anpasst. Die EAP-Messages werden hierzu in 802.1X-Messages verpackt (EAP over LAN – EAPOL). Ziel dieses Standards ist die portbezogene Zugangskontrolle in Netzwerken (Port-Based Network Access Control). An einer solchen portbezogenen Authentifizierung sind drei Elemente beteiligt:

- der Client (Supplicant), der sich in einem Netzwerk authentifizieren möchte,
- der Authentifizierer (Authenticator), der den Authentifizierungsvorgang mit dem Client durchführt, und
- der Authentifizierungs-Server (Authentication Server), der dem Authentifizierer die zur Authentifizierung erforderlichen Informationen zur Verfügung stellt.

## 2.3.11 IEEE802.1X im Detail

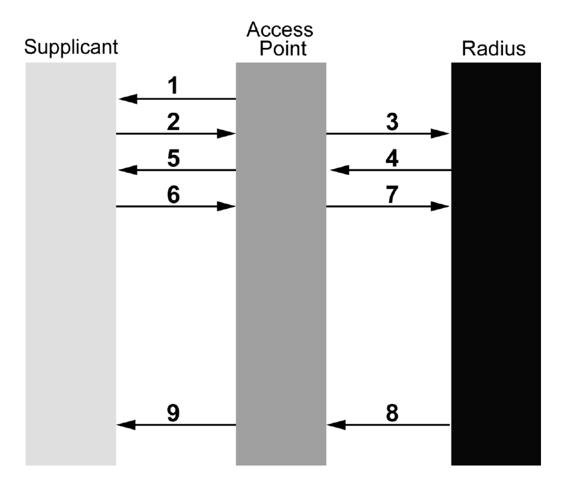
Die Idee hinter IEEE802.1X ist, dass einem physischen Anschluss zwei logische Anschlüsse (Ports) zugeordnet werden. Der physische Anschluss leitet die empfangenen Pakete grundsätzlich an den so genannten freien Port (Uncontrolled Port) weiter. Der kontrollierte Port (Controlled Port) kann nur nach einer Authentifizierung erreicht werden, die über den freien Port erfolgen kann.

In der Regel übernimmt ein RADIUS-Server (Remote Access Dial-Up User Service – RFC 2138) die Rolle des Authentifizierungs-Servers. Das RADIUS-Protokoll wurde ebenfalls zur Authentifizierung von Benutzern ausgerichtet, die sich über einen Wählzugang in einem Netzwerk anmelden wollen. Eine Beschreibung findet sich in den RFC 2138 und 2139 sowie 2865 bis 2868. Die EAP-Message wird dann als Attribut im RADIUS-Protokoll übertragen.

Für den Einsatz in einem WLAN ergibt sich folgender Ablauf, den Sie auch im nebenstehenden Bild nachvollziehen können:

1. Der Access Point fordert vom Client seine Identität.
2. Der Client liefert seine Identität an den Access Point.
3. Die Information über den offenen Port leitet der Access Point an den RADIUS-Server weiter.
4. Eine Authentifizierung des Client wird vom RADIUS-Server gefordert. Diese Anforderung (Challenge) sendet er zunächst an den Access Point.
5. Weiterleitung der Anforderung vom Access Point an den Client.
6. Der Client sendet eine Antwort auf die Anforderung an den Access Point. Sie enthält die geforderte Authentifizierung, etwa ein bestimmtes Passwort oder eine korrekte Verschlüsselung einer im Request enthaltenen Zeichenfolge.
7. Die Antwort leitet der Access Point an den RADIUS-Server weiter.
8. Der RADIUS-Server überprüft die Antwort. Im Fall eines Erfolgs sendet er eine entsprechende Meldung an den Access Point.

9. Der kontrollierte Port wird vom Access Point freigegeben. Darüber hinaus leitet er die Meldung an den Client weiter.




**Nutzererkennung:** Ablauf der Client-Authentifizierung im WLAN an einem RADIUS-Server.

## 2.3.12 Lücken in IEEE802.1X

IEEE802.1X stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netzwerke dar. Dennoch gibt es zwei Einschränkungen:

Erstens sieht IEEE802.1X nur eine Authentifizierung des Client vor, indem der Access Point den Verkehr über den kontrollierten Port erst nach der erfolgreichen Authentifizierung freigibt. Der Access Point selbst braucht seine Identität nicht nachzuweisen. Dies öffnet den Weg für einen Angriff eines „falschen Servers", der so genannten Man-in-the-Middle-Attack.

Zweitens enthalten nach einer einmal erfolgten Authentifizierung die einzelnen Pakete keine Zuordnung mehr. Daher kann im Rahmen eines so genannten Session Hijacking ein Angriff erfolgen, indem eine andere Station dem erfolgreich authentifizierten Client eine Disassociate-Meldung sendet, die diesen zur Beendigung der Verbindung auffordert. Der Access Point behält aber den kontrollierten Port weiterhin offen, so dass der Angreifer einen Zugang zum Netzwerk erhalten kann.

Solche Angriffe sind bei einer Dial-Up-Verbindung nicht praktikabel, da dabei die Serverseite durch die Verfügbarkeit unter einer festen Telefonnummer bereits authentifiziert ist. Bei fest verdrahteten und entsprechend nach außen abgesicherten Netzwerken erscheint das Risiko ebenfalls vergleichsweise gering.

## 2.3.13 Erweiterungen

Bei drahtlosen Netzwerken sind die bisher diskutierten Konzepte nicht ausreichend, was eine Reihe von Erweiterungen erforderlich macht. Zum einen erscheint eine wechselseitige Authentifizierung (Mutual Authentication) unabdingbar. Zu den bekanntesten Verfahren mit wechselseitiger Authentifizierung zählen unter anderem:

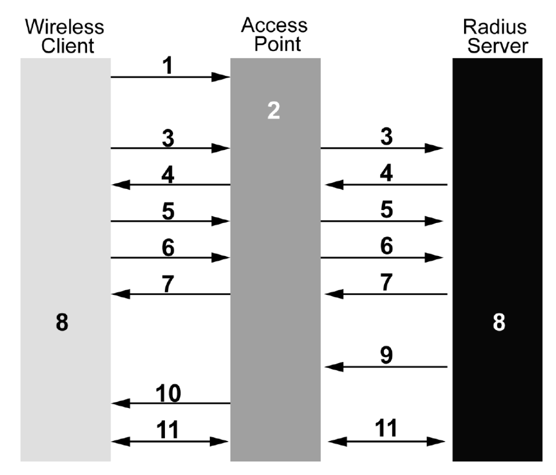
- das EAP-Transport Level Security (EAP-TLS in RFC 2716),
- das PPP Challenge Handshake Authentication Protocol (CHAP in RFC 1994) und die Microsoft-Implementierung, das Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), sowie
- das Lightweight EAP (LEAP), das vor allem Cisco unterstützt.

Zum anderen muss eine sichere Verschlüsselung der Pakete erfolgen, so dass weder ein Abhören der Nachrichten noch ein aktives Eindringen in das Netzwerk möglich ist. Als Beispiel für eine solche Verwaltung wird im Folgenden die Lösung vorgestellt, die Cisco für seine Produkte anbietet. Hierbei handelt es sich um eine Erweiterung eines Proxy-Servers, der die Rolle eines RADIUS-Servers übernimmt. Dieser Server wird von Cisco als ACS (Access Control Server) bezeichnet. Er verwendet für die Authentifizierung der WLAN-Terminals das MS-CHAP2 in Verbindung mit LEAP.

## 2.3.14 MS-CHAP2 mit LEAP

Eine Anmeldung beim Cisco-Access-Control-Server umfasst folgende Schritte:

1. Der IEEE802.11-Client meldet sich über den Uncontrolled Port beim Access Point an.
2. Der AP blockiert alle Requests des Client über den Controlled Port (zum Beispiel IP Requests), bis dieser sich am Netzwerk angemeldet hat.
3. Der User am IEEE802.11-Client meldet sich über seine normale Netzwerkanmeldung (Network Logon) mit Username und Passwort beim Radius-Server an, wobei der Access Point diese Anfrage weiterleitet.
4. Der Radius-Server authentifiziert den User. Hierzu wird ein MD5-Hash-Paket (Message Digest) mit einem zu verschlüsselnden Text (Challenge Text) über den Access Point an den Client übertragen.
5. Der Client sendet seine Antwort (Response) über den Access Point an den Radius-Server.
6. Auf diese Weise kann auch der Client den Radius-Server authentifizieren. Er sendet einen zu verschlüsselnden Text über den Access Point an den Radius-Server.
7. Der Radius-Server sendet seine Antwort (Response) über den Access Point an den Client.




**Proxy-Erweiterung:** Beim Cisco-Access-Control-Server erfolgt eine sichere Verschlüsselung der Pakete, so dass weder ein Abhören der Nachrichten noch ein aktives Eindringen in das Netzwerk möglich ist.

8. Radius-Server und Client berechnen den Session Key, der für die WEP-Verschlüsselung eingesetzt wird. Dieser wird berechnet mit Hilfe des User-Passworts und der Challenge Requests und Responses von Client und Server.
9. Der Radius-Server sendet den Session Key an den AP.
10. Der AP verschlüsselt seinen Broadcast-Key mit dem Session Key und sendet ihn an den Client.
11. Radius-Server und Client haben sich wechselseitig authentifiziert und verfügen nun ebenso wie der Access Point über einen User- und sitzungsspezifischen Schlüssel. Die verschlüsselte Datenübertragung kann also beginnen.

Dabei ist hervorzuheben, dass die Übertragung der Broadcast-Schlüssel bereits gesichert mit Hilfe des Session-Key erfolgt. Dieser kann durch die Rückführung auf Usernamen und Passwörter ohne manuellen Verwaltungsaufwand erzeugt werden. Zudem können die WEP-Schlüssel periodisch geändert werden.

Über die beschriebenen Gegenmaßnahmen hinaus können umfassende und bereits bestehende Sicherheitskonzepte auf den höheren Protokollebenen eingesetzt werden. Insbesondere bietet das Konzept der Virtuellen Privaten Netzwerke (VPN) einen sinnvollen Rahmen. VPNs basieren auf dem so genannten Tunneling, schließen aber Sicherheitsmechanismen wie Firewalls, Authentifizierung und Verschlüsselung als integrale Bestandteile mit ein.

## 2.3.15 Fazit

Wireless-LANs können auf der Grundlage der beschriebenen Sicherheitsmechanismen zuverlässig abgesichert werden – zumindest was die heutigen Angriffstechniken betrifft. Dies setzt aber voraus, dass die bereitstehenden Sicherheitsmaßnahmen auch tatsächlich umgesetzt werden. Dabei ist die Situation weiterhin dadurch geprägt, dass

- die verfügbaren Lösungen proprietär sind und somit nur in einer homogenen Umgebung umgesetzt werden können,
- ein Teil der Lösungen (RADIUS-Server, VPN) zwar praktikabel für größere Unternehmensnetze ist, für SoHo-Netzwerke allerdings kaum realisierbar erscheint. Heimnetzwerker sollten daher:
- eine vorhandene Verschlüsselung unbedingt nutzen.
- den statischen Schlüssel in regelmäßigen Abständen aktualisieren,
- eventuell vorhandene neue Treiber mit aufwendigerer Verschlüsselung, die über den Standard hinausgeht, vom Hersteller herunterladen,
- WLANs eine eigene SSID geben und ein SSID-Broadcast unterbinden,
- Zugangskontrolllisten auf MAC-Ebene pflegen und
- die Log-Dateien regelmäßig auf unbekannte MAC-Adressen überprüfen, um eventuelle Eindringversuche zu entdecken.

Bei größerem Engagement lässt sich auch über ein Auftrennen des Netzwerks in einen WLAN- und einen „sicheren“ Teil nachdenken, wobei die Kopplung über eine Firewall erfolgen kann. Diese Maßnahmen verringern das Risiko eines Eingriffs signifikant, auch wenn weiterhin Sicherheitslücken bleiben.

Axel Sikora

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| 802.11: Standard für drahtlose Netze | a680 | – |
| Test: Funknetze nach IEEE 802.11 | a620 | – |
| Wireless LANs im Überblick | a750 | – |
| Bluetooth – der Kabel-Killer | a477 | – |
| DECT: Die Alternative zu Bluetooth | a511 | – |
| Elektrosmog: Gefahren durch Mobilfunk? | a628 | – |

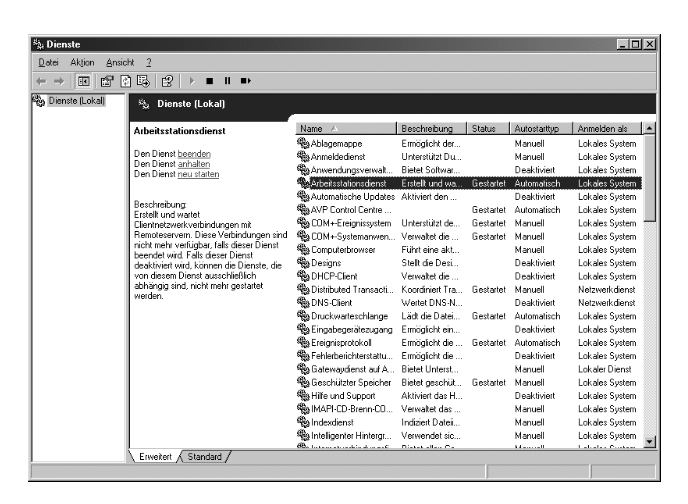
# 3 Client-Sicherheit

Trotz aller Absicherung von Netzwerk und Servern stellen die Client-Rechner im LAN immer noch einen bedeutenden Risikofaktor dar. Dies gilt speziell dann, wenn sie freien Zugang zum Internet haben. Über Bugs im Browser gelangen Schädlinge oder Trojaner auf den Rechner des Mitarbeiters und von dort ins gesamte LAN. Wie Sie die Client-Rechner absichern und die Mitarbeiter auf die potenziellen Gefahren hinweisen, zeigt dieser Abschnitt des Compact.

## 3.1 XP-Dienste aufräumen

Windows XP beansprucht Ressourcen für Gimmicks und Dienste, die nicht jeder braucht. Mit einer optimierten Konfiguration läuft XP auch auf älteren PCs rund. Professionelle Anwender profitieren von mehr Sicherheit.

Um es auch dem unbedarftesten Benutzer leicht zu machen, installiert und startet Windows XP eine ganze Reihe von Diensten, selbst wenn sie gar nicht benötigt werden. Zwar zeigt das System dabei eine rudimentäre „Grundintelligenz“. So richtet es beispielsweise die Infrarot-Überwachung nur auf Geräten ein, die auch über einen Infrarot-Adapter verfügen. Allerdings hat Microsoft diese Plausibilitätsprüfung vor der Aktivierung eines Dienstes nicht so sorgfältig und konsequent implementiert, wie man es sich wünschen würde.




**Wenig hilfreich:** Die Beschreibung eines Dienstes hilft nicht gerade bei der Entscheidung, ob er notwendig ist oder nicht.

So erscheint es als äußerst fragwürdig, dass die „Konfigurationsfreie drahtlose Verbindung“ auf jedem Rechner installiert und gestartet wird – unabhängig davon, ob er auch über einen 802.11b-Adapter verfügt. Ebenso merkwürdig ist, dass der Dienst „Designs“ nicht automatisch gestoppt wird, selbst wenn der Benutzer auf die klassische Windows-Oberfläche (**webcode: a666**) umschaltet.

Mit einer geschickten Auswahl der Dienste lassen sich zum einen Speicher- und Prozessorressourcen sparen, so dass XP auch auf älteren Systemen einsetzbar ist. Bei einem Upgrade im Firmennetz macht sich das schnell bemerkbar, wenn man nicht gezwungen ist, Hunderte von Rechnern mit neuer Hardware auszurüsten. Besonders wichtig ist gerade für den Firmeneinsatz allerdings eine Verbesserung der Sicherheit, indem unbenötigte Dienste wegfallen und somit selbst bei Vorhandensein von Sicherheitslücken eine Ausnutzung derselben nicht möglich ist.

Der Dienste-Manager von XP gibt zwar grundlegend Auskunft über den Dienst und darüber, was er tut. Er bietet jedoch kaum Hilfestellung bei der Frage, ob dieser Dienst notwendig ist oder nicht. Oft verwirrt er sogar durch den lapidaren nichts sagenden Hinweis: „Falls dieser Dienst deaktiviert wird, können die Dienste, die von diesem Dienst ausschließlich abhängig sind, nicht mehr gestartet werden.“

### 3.1.1 Unverzichtbare Dienste

So sehr man das Angebot zusammenstreichen kann, eine Handvoll der Windows-Dienste ist tatsächlich unverzichtbar für einen reibungslosen Betrieb. Dazu gehört beispielsweise der RPC-Dienst, von dem so ziemlich alle weiteren Systemkomponenten abhängen, wie etwa auch COM. Wer auf Sound nicht verzichten kann, sollte „Windows Audio“ nicht abschalten und darf infolgedessen auch „Plug&Play“ nicht deaktivieren.

Um zu drucken, ist die Druckerwarteschlange unabdingbar, und in Windows-Netzen kommt man nicht ohne den Arbeitsstationsdienst aus. Dieser sorgt unter anderem dafür, dass die Verbindungen zu den anderen Rechnern hergestellt werden.

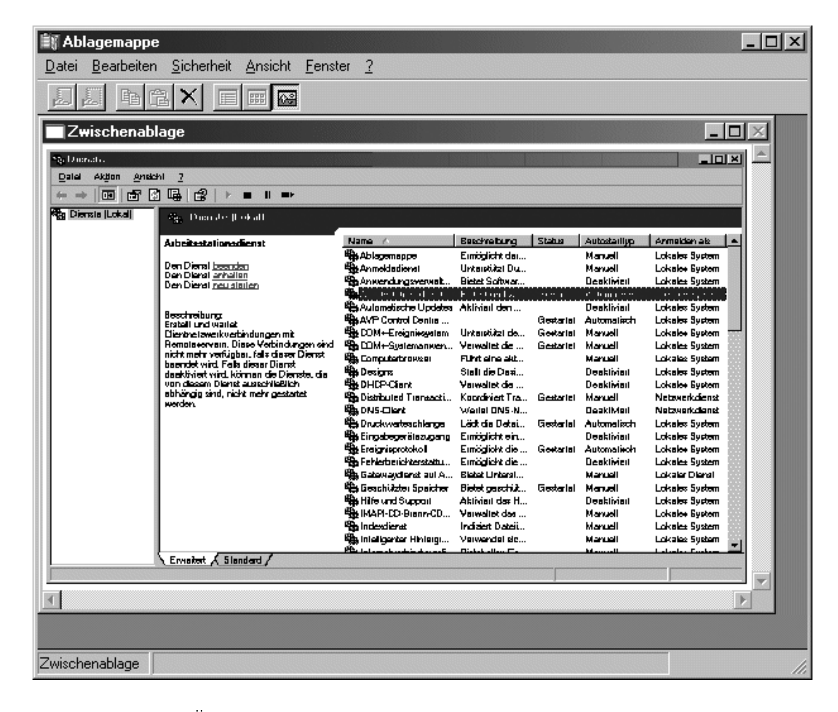
Das Ereignisprotokoll und die „Windows Verwaltungsinstrumentation“ sollten Sie ebenfalls unangetastet lassen. Letztere ist unter anderem dafür zuständig, dass der Dienstemanager einwandfrei funktioniert. Auch bei der Sicherheitskontenverwaltung haben Sie keine Chance, Ressourcen zu sparen. Sie ist integraler Bestandteil des Sicherheitsmodells von Windows XP, inklusive der Rechteverwaltung.

Die Kryptographiedienste verwalten Zertifikate und Stammstellen und sorgen dafür, dass Signaturen von Windows-Dateien bestätigt werden können. Ohne diesen Dienst funktioniert unter anderem auch das automatische Windows-Update über die entsprechende Website von Microsoft nicht mehr.

Alle übrigen Dienste sind in der einen oder anderen Umgebung nicht erforderlich und können dementsprechend ohne großes Risiko abgeschaltet werden. Um welche Dienste es sich dabei handelt und unter welchen Bedingungen man auf sie verzichten kann, lesen Sie auf den nächsten Seiten.

## 3.1.2 Ablagemappe

Dieser Dienst ermöglicht es der Ablagemappe, Informationen zu speichern und mit anderen Computern im Netzwerk auszutauschen. Da der Starttyp dieses Services per Default auf manuell steht, gibt es hier keinen Handlungsbedarf.




**Verteilzentrum:** Über die Ablagemappe können Sie Inhalte der Zwischenablage für andere Nutzer im Netz freigeben. Wenn Sie verhindern wollen, dass durch Bugs oder Viren möglicherweise ein Sicherheitsloch geöffnet wird, dann sollten Sie diesen Dienst deaktivieren.

## 3.1.3 Anmeldedienst

Der Anmeldedienst unterstützt eine Durchsatzauthentifizierung von Kontoanmeldungsereignissen für Computer innerhalb einer Domäne. Dieser Dienst wird daher nur in einer Windows-Domäne, und auch dort nur für die eigentliche Anmeldung benötigt. Allerdings ist ohne ihn die Anmeldung an eine Windows-Domäne nicht mehr möglich.

### 3.1.4 Anwendungsverwaltung

Die Anwendungsverwaltung bietet Software-Installationsdienste wie Zuweisung, Veröffentlichung und Deinstallation. Dieser Dienst wird nur gestartet, wenn eine Systemkomponente Zugriff auf die in Windows eingebauten Installationsfunktionen benötigt, etwa um eine Software einzurichten.

### 3.1.5 Arbeitsstationsdienst

Der Arbeitsstationsdienst erstellt und wartet Client-Netzwerkverbindungen mit entfernten Servern. Solche Verbindungen sind nicht mehr verfügbar, falls der Dienst beendet wird.

In einer Netzwerkumgebung sollte man diesen Dienst nicht beenden, da ansonsten keine Verbindungen mehr zu Rechnern oder Shares im Netzwerk aufgebaut werden können.

### 3.1.6 Automatische Updates

Dieser Dienst aktiviert den automatischen Download und die Installation für wichtige Aktualisierungen von Windows Update. Wer Bedenken hegt, dass Microsoft bei dieser Gelegenheit möglicherweise Daten ausspionieren könnte, sollte den Dienst deaktivieren.

Aktuelle Patches und Bugfixes finden sich auch auf der Windows-Update-Website von Microsoft (http://windowsupdate.microsoft.com). Dort wird allerdings ein ActiveX-Control installiert, das den Rechner inspiziert und anschließend entsprechende Patches zum Download anbietet.

Wer ganz sichergehen will, holt die gewünschten Aktualisierungen ausschließlich von der Update-Seite für Firmenkunden (http://v4.windowsupdate.microsoft.com /catalog/de/), denn diese untersucht die lokale Software nicht.

Bei beiden Update-Seiten gilt: Sie müssen sie mit dem richtigen Betriebssystem besuchen. Gehen Sie mit Windows 2000 auf die Seite, erhalten Sie auch nur Patches für dieses Betriebssystem.

### 3.1.7 COM+-Ereignissystem

COM+ unterstützt den Systemereignis-Benachrichtigungsdienst (SENS, System Event Notification Service), der die automatische Verteilung von Ereignissen an abonnierende COM-Komponenten zur Verfügung stellt.

Wenn Sie diesen Dienst beenden, wird gleichzeitig auch die System Event Notification beendet. Das System ist dann nicht mehr in der Lage, den einzelnen Abonnenten Anmelde- und Abmeldebenachrichtigungen zur Verfügung zu stellen.

Über das COM+-Ereignissystem können Systemkomponenten sich automatisch informieren lassen, wenn ein bestimmtes Systemereignis auftritt. Derzeit wird dieser Dienst primär von SENS genutzt. Wenn Sie also den System Event Notification Service nutzen wollen, deaktivieren Sie diesen Dienst nicht.

### 3.1.8 Computer-Browser

Dieser Dienst führt eine aktuelle Liste aller Computer im Windows-Netzwerk und gibt sie an als Browser fungierende Computer weiter. Die Liste wird nicht aktualisiert oder gewartet, falls Sie den Dienst beenden.

Er ist nur in einem Netzwerk sinnvoll, lässt sich aber auch da auf Arbeitsrechnern deaktivieren, solange ein Server im Netz diesen Dienst anbietet. Um den Serverdienst abzuschalten, müssen Sie auch diesen Dienst deaktivieren.

### 3.1.9 Designs

Dieser Dienst ist für die Luna-Oberfläche (**webcode: a666**) zuständig. Er wird allerdings nicht automatisch abgeschaltet, auch wenn Sie auf die klassische Windows-Oberfläche umschalten. Um Speicher und Ressourcen zu sparen, können Sie ihn gefahrlos deaktivieren.

### 3.1.10 DFÜ-Netzwerk und Konsorten

Eine ganze Reihe von Diensten ist erforderlich, wenn per Wählverbindung eine Internet-Verbindung aufgebaut wird. Das ist nicht nur bei Modem oder ISDN der Fall, sondern auch bei direkter DSL-Anwahl per PPPoE.

Hier werden dann die Dienste „RAS-Verbindungsverwaltung“, „Telefonie“, „Verwaltung für automatische RAS-Verbindung“ sowie gegebenenfalls „Internetverbindungsfirewall/Gemeinsame Nutzung der Internetverbindung“ und „Gatewaydienst auf Anwendungsebene“ benötigt.

Bauen Sie dagegen die Internet-Verbindung über ein LAN und einen Router auf, können Sie getrost auf diese Dienste verzichten und sie komplett abschalten.

### 3.1.11 DHCP-Client

Der DHCP-Client ist nur notwendig, wenn Sie einen DHCP-Server (**webcode: a206**) in Ihrem Netzwerk einsetzen. Ansonsten müssen Sie die TCP/IP-Einstellungen für die Netzwerkkarte ohnehin fest einstellen. Dennoch installiert und aktiviert Windows XP diesen Dienst. Auch hier können Sie den Dienst gefahrlos und ohne Nachteile abschalten.

### 3.1.12 DNS-Client

Der DNS-Client speichert Anfragen an einen DNS-Server (**webcode: a205**) zwischen, so dass die IP-Adresse (**webcode: a209**) bei späteren Anfragen schneller gefunden wird. In schnellen Netzwerken oder bei DSL-Verbindungen ist das nicht unbedingt erforderlich, mitunter nachteilig: Da nicht einstellbar ist, wie lange ein Domain-Name im Cache verbleibt, gibt der DNS-Client eventuell eine falsche IP-Adresse zurück, wenn ein Server plötzlich eine andere Adresse hat. Für langsame Internet-Anbindungen, wie etwa per Modem, kann dieser Dienst sich jedoch als hilfreich erweisen.

### 3.1.13 Fehlerberichterstattung

Über diesen Dienst will sich Microsoft bei Programmabstürzen informieren lassen, um das Problem einzugrenzen. Stürzt ein Programm mit einer Fehlermeldung ab, bietet Windows dem Anwender gleich an, ein Fehlerprotokoll an Microsoft zu schicken. Dieses enthält unter anderem einen Abzug des Hauptspeichersegments, in dem der Fehler aufgetreten ist.

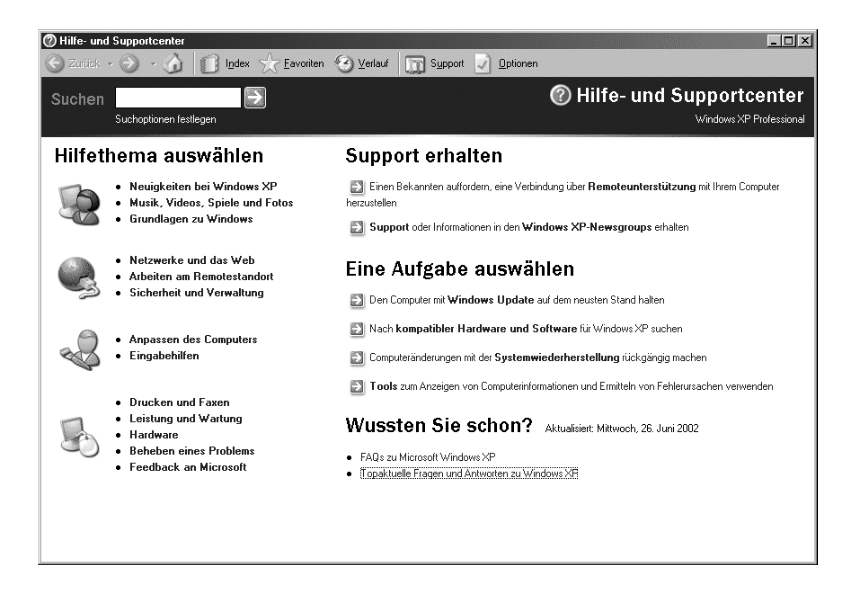
Für Microsoft und die Fehlerbehebung mag das hilfreich sein, aber der sicherheitsbewusste Anwender macht sich eventuell Sorgen um seine Privatsphäre. Deshalb sollten Sie diesen Dienst deaktivieren. Das erfolgt entweder über den Dienstemanager oder die Eigenschaften des Arbeitsplatzes im Reiter „Erweitert“.

### 3.1.14 Geschützter Speicher

Dieser Dienst bietet geschützten Speicherplatz für private Daten, wie beispielsweise private Schlüssel, um den Zugriff durch nicht autorisierte Dienste, Prozesse oder Benutzer zu unterbinden. Wird dieser Dienst deaktiviert, kann beispielsweise Outlook keine Kennwörter mehr speichern. Sie müssten also für jeden Anmeldevorgang das E-Mail-Passwort neu eingeben. Außerdem kann der Internet Explorer dann keine Formularfelder oder Benutzernamen und Passwörter speichern.

### 3.1.15 Hilfe und Support

Aktiviert das Hilfe- und Supportcenter auf dem Computer. Laut Beschreibung im Dienstemanager ist das Hilfe- und Supportcenter nicht verfügbar, wenn dieser Dienst beendet wird. Das stimmt allerdings nicht ganz: Ruft man über das Startmenü „Hilfe und Support“ auf, startet Windows XP den Dienst. Unabhängig davon, ob er deaktiviert ist oder nicht – eigentlich dürfte es nicht passieren, dass ein deaktivierter Dienst vom System gestartet wird. Zudem setzt Windows ihn ungefragt wieder auf den Starttyp „automatisch“.




**Eigenmächtig:** Ruft man die Windows-Hilfe auf, startet XP den Dienst „Hilfe und Support" – auch wenn dieser deaktiviert ist.

Dementsprechend ist es kein Problem, diesen Dienst zu deaktivieren. Sie sollten lediglich nicht vergessen, ihn wieder abzuschalten, sobald Sie einmal die Windows-Hilfe aufgerufen haben.

## 3.1.16 Infrarot-Überwachung

Auf Rechnern mit einer Infrarot-Schnittstelle ist dieser Dienst per Default aktiv. Er stellt die Unterstützung für die installierten Infrarot-Geräte bereit und sucht nach anderen Geräten in Reichweite, um automatisch eine Verbindung aufzubauen.

Da jedoch die IrDA-Schnittstelle im Regelfall nur hin und wieder tatsächlich benötigt wird, reicht es auch, den Dienst auf „manuell" zu stellen und bei Bedarf über den Dienstemanager zu starten.

## 3.1.17 Internet-Verbindungsfreigabe

Über einen Windows-Rechner lässt sich gegebenenfalls die Internet-Verbindung auch für andere Windows-Rechner im lokalen Netzwerk freigeben. Dieses Internet Connection Sharing (ICS) benötigt jedoch eine ganze Reihe von Diensten zur reibungslosen Funktion.

Der eigentliche Dienst („Internetverbindungs-Firewall“) hängt unter anderem vom Gateway-Dienst auf Anwendungsebene (Application Layer Gateway – ALG), den Netzwerkverbindungen (Netman), NLA (Network Location Awareness) sowie der RAS-Verbindungsverwaltung (siehe: DFÜ-Netzwerk und Konsorten **webcode: 944p10**) ab.

### 3.1.18 IPSEC-Dienste

Über die Internet Protocol Security Suite (IPsec) sichert und kontrolliert Windows XP die Übertragung von IP-Paketen. IPSEC zeichnet dabei zuständig für die Überprüfung, die Authentifizierung und gegebenenfalls die Verschlüsselung der Daten. Allerdings braucht nicht jeder die IPSEC-Dienste, dennoch werden sie von Windows XP automatisch gestartet.

Dass sie dennoch von Microsoft auf Client-Rechnern nicht unbedingt vorgesehen sind, zeigt die Tatsache, dass die entsprechende Konfiguration gut versteckt ist. Im normalen Verwaltungsmenü taucht sie gar nicht erst auf. Sie müssen sie gesondert aufrufen, indem Sie die Management-Konsole (mmc.exe) starten und dann das IPSEC-Snap-in manuell hinzufügen.

### 3.1.19 Schnelle Benutzerumschaltung

Eine der Neuerungen von Windows XP ist die so genannte „schnelle Benutzerumschaltung“. Dabei kann sich ein anderer Benutzer auf dem Rechner anmelden, ohne zunächst einen eventuell eingeloggten Benutzer abzumelden. Dessen Programme laufen also weiterhin im Hintergrund.

Diese Lösung verbraucht jedoch eine ganze Menge Speicher und kommt nur selten wirklich zum Einsatz. Auf Rechnern mit weniger als 128 MByte Speicher ist sie denn auch gar nicht erst eingeschaltet, auf Rechnern mit mehr Speicher aktiviert Microsoft sie allerdings per Default. Sie können die „schnelle Benutzerumschaltung“ jedoch im Applet *Benutzerkonten der Systemsteuerung* oder über den Dienstemanager jederzeit deaktivieren.

### 3.1.20 Konfigurationsfreie drahtlose Verbindung

Bei drahtlosen Netzwerken nach IEEE 802.11b (**webcode: a620**) müssen Sie die SSID des Access Point konfigurieren, über den Sie ins Netzwerk möchten. Windows XP will es dem Anwender dabei leichter machen und startet deswegen den Dienst für eine „Konfigurationsfreie drahtlose Verbindung“.

Dieser Service konfiguriert die WLAN-Karte auf die SSID „any“ und listet dann alle verfügbaren drahtlosen Netzwerke auf. Aus der so erstellten Liste kann der Anwender anschließend auswählen, in welches Netz er sich einbuchen will.

Dieser Dienst ist zwar an sich ganz nützlich. Wenn man allerdings nicht ständig in wechselnden WLANs unterwegs ist, benötigt man ihn nicht unbedingt. Beim Deaktivieren ist allerdings zu beachten, dass die XP-Treiber für WLAN-Karten häufig nicht mehr die Option bieten, eine SSID zu konfigurieren.

Mitunter hilft es, die Windows-2000-Treiber oder zumindest ein entsprechendes Control-Applet für die WLAN-Karte zu verwenden. Funktioniert beides nicht, können Sie den Dienst nicht abschalten. Wenn Sie ohnehin keine WLAN-Karte im Rechner haben, lässt sich der Dienst ohne Nachteile deaktivieren.

### 3.1.21 Nachrichtendienst

Der Nachrichtendienst überträgt Nachrichten, die mit dem Befehl *net send* oder über eine entsprechende API verschickt werden. Dies ist in manchen Software-Umgebungen noch immer ein gängiges Mittel, um Warnungen an den Administrator oder einzelne Benutzer zu versenden.

In den meisten Fällen wird der Dienst allerdings nicht mehr benötigt, so dass Sie ihn getrost abschalten können. Auch wenn der Kurzname des Dienstes „Messenger“ lautet, hat er nichts mit dem Microsoft Messenger zu tun, der automatisch mit Windows XP installiert wird.

Da zunehmend Spam über den Befehl *net send* verschickt wird, empfiehlt es sich, den Dienst abzuschalten.

### 3.1.22 Remote Desktop

Windows XP bietet gleich eine ganze Reihe von Diensten an, die den Fernzugriff auf Desktops ermöglichen.

Zum einen ist das die Netmeeting-Remotedesktop-Freigabe, mit der ein anderer Netmeeting-Benutzer auf den eigenen Desktop zugreifen kann. Da dieses ein potenzielles Sicherheitsloch darstellt, empfehlen wir dringend die Änderung des Startmodus auf „deaktiviert“. Zur Erinnerung: „Manuell“ heißt, dass dieser Dienst von einem anderen Dienst oder Programm gestartet werden könnte, ohne dass Sie davon etwas mitbekommen.

Auch der Sitzungsmanager für Remotedesktophilfe ermöglicht den Zugriff auf den Desktop des Benutzers. Normalerweise steuern Sie diesen Dienst über Systemeigenschaften/Remote. Allerdings ist es angebracht, ihn komplett zu deaktivieren, um einen ungewollten Start zu verhindern.

Eine erweiterte Form der Remotedesktophilfe stellen die Terminaldienste dar. Sind diese gestartet, kann auch ohne „Unterstützungsanforderung“ eine Sitzung zum eigenen Rechner aufgebaut werden. Unter gewissen Umständen macht das durchaus Sinn – etwa wenn man von der Arbeitsstelle aus auf den Rechner zu Hause zugreifen möchte. In den meisten Fällen öffnet diese Möglichkeit jedoch

schlicht eine potenzielle Sicherheitslücke. Falls Sie allerdings die „Schnelle Benutzerumschaltung“ (**webcode: 944p18**) verwenden wollen, benötigen Sie dazu die Terminaldienste zwingend.

## 3.1.23 Remote-Dienste

Mit der Remote-Registrierung – sie ist in Windows XP Home nicht enthalten – ermöglichen Sie den Fernzugriff auf die in der Registry enthaltenen Einstellungen. Eine Änderung des Starttyps von „manuell“ auf „deaktiviert“ scheint daher nicht nur bei paranoiden Administratoren angeraten.

Weitere potenzielle Angriffspunkte stellen die ebenfalls selten benötigten Netzwerk-DDE-Dienste (Client und Server) dar. Sie ermöglichen den Netzwerktransport für dynamischen Datenaustausch, so dass auch DDE-Verbindungen zwischen Anwendungen auf verschiedenen Rechnern möglich sind. Der Serverdienst verwaltet entsprechende DDE-Freigaben im Netzwerk.

## 3.1.24 Server

Der Serverdienst ist für Datei- und Druckerfreigaben zuständig. Auch wenn Sie auf Ihrem Rechner keine Freigaben eingerichtet haben, startet Windows XP diesen Dienst. Um ihn abschalten zu können, müssen Sie zudem den Dienst Computerbrowser beenden und deaktivieren.

## 3.1.25 Systemereignisbenachrichtigung

Dieser Dienst verfolgt Systemereignisse wie Windows-Anmeldungen sowie Netzwerk- und Stromversorgungsereignisse. Er informiert außerdem Ereignissystembezieher von COM+ über diese Ereignisse.

Für Notebook-Besitzer ist dieser Dienst beinahe zwingend erforderlich, da er unter anderem dafür sorgt, dass bei niedrigem Batteriestand die konfigurierten Aktionen ausgeführt werden. In einer Desktop-Umgebung ist uns derzeit kein Umfeld bekannt, in dem die Systemereignisbenachrichtigung unbedingt benötigt wird.

## 3.1.26 Upload-Manager

Die im Dienstemanager hinterlegte Beschreibung dieses Service lautet wie folgt: „Verwaltet synchrone und asynchrone Dateiübertragungen zwischen Clients und Servern im Netzwerk. Synchrone und asynchrone Dateiübertragungen zwischen Clients und Servern werden nicht ausgeführt, wenn dieser Dienst beendet wird.“ Diese Formulierung vermittelt zwangsläufig den Eindruck, dass ohne den Upload-Manager kein einziges Datenpaket über das Netzwerk fließen würde.

Tatsächlich läuft auf unseren Testsystemen jedoch der Netzwerkverkehr auch nach dem Abschalten des Upload-Managers ohne offensichtliche Beeinträchtigung von Funktionen normal weiter.

### 3.1.27 UPnP-Dienste

Mit Universal Plug-and-Play hat Microsoft eine neue Funktion eingeführt, die im Netz ungefähr das leisten soll, was PnP auf dem lokalen Rechner bietet: Die automatische Erkennung neuer Dienste und Geräte (Drucker, Freigaben et cetera). Zusätzlich kann Windows XP diese Dienste ins Internet bereitstellen, auch wenn der anbietende Rechner durch NAT für das Internet unsichtbar ist.

Da UPnP bereits durch eine schwer wiegende Sicherheitslücke glänzte und es generell fraglich ist, ob man diesen Dienst wirklich braucht, empfiehlt sich die Deaktivierung. Zwei Teildienste sind für UPnP zuständig: Der UPnP-Geräte-Host lässt den Rechner als Host für entsprechende Geräte im Netzwerk fungieren, der SSDP-Suchdienst ist für das Aufspüren dieser Geräte zuständig.

### 3.1.28 WebClient

Der WebClient ermöglicht es Programmen, Internet-basierte Dateien zu erstellen, darauf zuzugreifen und sie zu verändern. Wenn dieser Dienst beendet wird, werden diese Funktionen nicht mehr zur Verfügung stehen. Solange Sie keine Software mit WebDAV-Funktionen verwenden (etwa Microsoft Frontpage), können Sie diesen Dienst ausschalten.

### 3.1.29 Windows-Zeitgeber

Ein weiterer Dienst, dem des Öfteren Spionage-Funktionen nachgesagt werden, ist der automatische Uhrenabgleich mit Internet-Servern. Der Windows-Zeitgeber verbindet sich mit einem entsprechenden Dienst auf einem Rechner, der mit einer Atomuhr (etwa über Funk) synchronisiert ist, und errechnet über verschiedene Algorithmen die Abweichung der lokalen Rechneruhr von der richtigen Zeit. Hier handelt es sich um ein standardisiertes Protokoll, Windows kann so gut wie gar nicht spionieren. Wer dennoch sicher sein will, sollte den Dienst deaktivieren.

### 3.1.30 Windows-Dienste im Überblick

In der folgenden Tabelle finden Sie alle von Microsoft installierten Windows-Dienste im Überblick. Die Angabe „Kurzname" enthält den Namen, den Sie verwenden müssen, um einen Dienst per Kommandozeilenbefehl „net start", „net pause" oder „net stop" zu verwalten.

Dienste mit dem Starttyp „automatisch“ werden beim Systemstart hochgefahren. „Manuell“ bedeutet, dass ein Dienst per „net start“, über den Dienstemanager oder auf Grund einer Abhängigkeit beim Laden eines anderen Dienstes startet. Deaktivierte Dienste laufen – abgesehen vom Dienst „Hilfe und Support“ – niemals.

Die Spalte Beschreibung enthält die Beschreibung aus dem Dienstemanager – allerdings ohne den jeweils überflüssigen Zusatz, dass sich abhängige Dienste nicht mehr starten lassen, wenn ein Dienst abgeschaltet wird.

Mike Hartmann

**Windows-Dienste im Überblick**

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Ablagemappe – ClipSrv | M/D | – | Ermöglicht der Ablagemappe, Informationen zu speichern und mit Remote-Computern auszutauschen. Wenn dieser Dienst beendet wird, wird die Ablagemappe keine Informationen mehr mit Remote-Computern austauschen können. |
| Anmeldedienst – Netlogon | M/M | – | Unterstützt Durchsatz-Authentifizierung von Kontoanmeldungsereignissen für Computer in einer Domäne. |
| Anwendungsverwaltung – ApPMgmt | M/M | – | Bietet Software-Installationsdienste wie Zuweisung, Veröffentlichung, und Deinstallation. |
| Arbeitsstationsdienst – lanman-workstation | A/A | Netlogon, Browser, BITS, Messenger, RpcLocator, Alerter | Erstellt und wartet Client-Netzwerkverbindungen mit Remote-Servern. Diese Verbindungen sind nicht mehr verfügbar, falls dieser Dienst beendet wird. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Automatische Updates – wuauserv | A/M | – | Aktiviert den Download und die Installation für wichtige Updates von Windows Update. Das Betriebssystem kann manuell über die Windows-Update-Website aktualisiert werden, falls der Dienst deaktiviert wird. |
| COM+-Ereignissystem – EventSystem | M/M | SENS | Unterstützt den Benachrichtigungsdienst für Systemereignisse (SENS, System Event Notification Service), der die automatische Verteilung von Ereignissen an abonnierende COM-Komponenten zur Verfügung stellt. Wenn der Dienst beendet ist, wird SENS deaktiviert und ist nicht in der Lage, Anmelde- und Abmeldebenachrichtigungen bereitzustellen. |
| COM+-Systemanwendung – COMSysApp | M/M | – | Verwaltet die Komponentenkonfiguration und -überwachung von COM+-basierten Komponenten. Nach dem Beenden des Dienstes sind die meisten COM+-basierten Komponenten nicht ordnungsgemäß funktionsfähig. |
| Designs – Themes | A/* | – | Stellt die Designverwaltung zur Verfügung. |
| DHCP-Client – Dhcp | A/* | – | Verwaltet die Netzwerkkonfiguration, indem IP-Adressen und DNS-Namen registriert und aktualisiert werden. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Distributed Transaction Coordinator – MSDTC | M/M | – | Koordiniert Transaktionen, die sich über mindestens zwei Ressourcenverwaltungen wie Datenbanken, Nachrichtenwarteschlangen oder Dateisysteme erstrecken. Wenn der Dienst beendet ist, treten diese Transaktionen nicht auf. |
| DNS-Client – Dnscache | A/* | – | Wertet DNS-Namen (Domain Name System) für diesen Computer aus und speichert sie zwischen. Falls dieser Dienst beendet wird, kann der Computer keine DNS-Namen auflösen und Active-Directory-Domänen-Controller ermitteln. |
| Druckerwarteschlange – Spooler | A/A | – | Lädt die Dateien in den Arbeitsspeicher, um sie später zu drucken. |
| Eingabegerätezugang – HidServ | D/D | – | Ermöglicht einen Standardeingabezugang für Eingabegeräte (HID-Geräte), welcher die Verwendung von vordefinierten Schnelltasten auf Tastaturen, Fernbedienungen und anderen Multimedia-Geräten aktiviert und unterstützt. Wenn dieser Dienst beendet wird, funktionieren die von ihm gesteuerten Schnelltasten nicht mehr. |
| Ereignisprotokoll – Eventlog | A/A | Winmgmt | Ermöglicht die Ansicht von Ereignisprotokollmeldungen von Windows-basierten Programmen und Komponenten in der Ereignisanzeige. Dieser Dienst lässt sich nicht beenden. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| **Dienstname – Kurzname** | **Starttyp Default/ Empfohlen** | **Abhängige Dienste** | **Beschreibung** |
|---|---|---|---|
| Fehlerbericht-ertattung – ERSvc | A/D | – | Ermöglicht die Fehlerbericht-erstattung für Dienste und Anwendungen, die in nicht standardgemäßen Umgebungen ausgeführt werden. |
| Gatewaydienst auf Anwendungs-ebene – ALG | M/M | SharedAccess | Bietet Unterstützung für Protokoll-Plug-ins von Drittanbietern für die gemeinsame Nutzung der Internet-Verbindung und der Internet-Verbindungs-Firewall. |
| Geschützter Speicher – Protected-Storage | A/A | – | Bietet geschützten Speicherplatz für private Daten, wie etwa private Schlüssel, um Zugriffe durch nicht autorisierte Dienste, Prozesse oder Benutzer zu unterbinden. Wird dieser Dienst deaktiviert, kann beispielsweise Outlook keine Kennwörter mehr speichern. |
| Hilfe und Support – helpsvc | A/M | – | Aktiviert das Hilfe- und Supportcenter auf diesem Computer. Das Hilfe- und Supportcenter ist nicht verfügbar, wenn dieser Dienst beendet wird. |
| IMAPI-CD-Brenn-COM-Dienste – ImapiService | M/M | – | Verwaltet das Aufnehmen von CDs mit IMAPI (Image Mastering Applications Programming Interface). Auf diesem Rechner können keine CDs aufgenommen werden, wenn dieser Dienst angehalten wird. |
| Indexdienst – cisvc | M/M | – | Indiziert Dateiinhalt und -eigenschaften auf lokalen und Remote-Computern und bietet schnellen Dateizugriff durch eine flexible Abfragesprache. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Infrarot-Überwachung – Irmon | A/* | – | Unterstützt auf dem Computer installierte Infrarot-Geräte und sucht nach anderen Geräten in Reichweite. |
| Intelligente Hintergrundübertragung – BITS | M/M | – | Verwendet für die Datenübertragung Netzwerkbandbreite, die sich in Leerlauf befindet. |
| Internetverbindungsfirewall – SharedAccess | M/M | – | Ermöglicht für alle Computer im Netzwerk Dienste für die Netzwerkadressübersetzung, Adressierung, Namensauflösung und Eindringschutz. |
| IPSEC-Dienste – PolicyAgent | A/* | – | Verwaltet IP-Sicherheitsrichtlinien und startet den IKE- (ISAKMP - Oakley) sowie den IP-Sicherheitstreiber. |
| Kompatibilität für schnelle Benutzerumschaltung – FastUser-Switching-Compatibility | A/* | – | Bietet Verwaltung für Anwendungen, die Unterstützung in einer Mehrbenutzerumgebung erfordern. |
| Konfigurationsfreie drahtlose Verbindung – WZCSVC | A/* | – | Bietet automatische Konfiguration für 802.11-Adapter. |
| Kryptografiedienste – CryptSvcs | A/A | – | Stellt drei Verwaltungsdienste bereit: Der Katalogdatenbankdienst bestätigt Dateisignaturen; der Dienst für geschützten Stammspeicher fügt Zertifikate vertrauenswürdiger Stammzertifizierungsstellen hinzu und entfernt sie; der Schlüsseldienst unterstützt den PC bei Einschreibungen in Zertifikate. Beendet man diesen Dienst, funktionieren die drei Verwaltungsdienste nicht korrekt. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Leistungsdatenprotokolle und Warnungen – SysmonLog | M/M | – | Sammelt nach einem vorkonfigurierten Zeitplan Leistungsdaten vom lokalen oder von Remote-Computern, schreibt die Daten in ein Protokoll oder löst Warnungen aus. Beendet man diesen Dienst, sammelt er keine Leistungsdaten mehr. |
| MS Software Shadow Copy Provider – SwPrv | M/M | – | Verwaltet Software-basierte Schattenkopien des Volume-Schattenkopie-Dienstes. Software-basierte Schattenkopien lassen sich bei beendetem Dienst nicht verwalten. |
| Nachrichtendienst - Messenger | A/* | – | Überträgt NET SEND- und Warndienstnachrichten zwischen Clients und Servern. Dieser Dienst ist nicht mit Windows Messenger verwandt. Der Warndienst überträgt keine Nachrichten, falls dieser Dienst beendet ist. |
| NetMeeting-Remote-Desktop-Freigabe – mnmsrvc | M/D | – | Ermöglicht einem autorisierten Benutzer an einem anderen Computer, auf diesen Rechner mit NetMeeting über ein Intranet zuzugreifen. Wird dieser Dienst beendet, ist die Remote-Desktop-Freigabe nicht mehr verfügbar. |
| Netzwerk-DDE-Dienst – NetDDE | M/D | ClipSrv | Ermöglicht Netzwerktransport und Sicherheit für den dynamischen Datenaustausch (DDE) von Programmen, die innerhalb des Computers oder auf verschiedenen Rechnern ausgeführt werden. Wird dieser Dienst beendet, stehen DDE-Transport und -Sicherheit nicht mehr zur Verfügung. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Netzwerk-DDE-Serverdienst – NetDDEsdm | M/D | NetDDE | Verwaltet die DDE-Netzwerkfreigaben (Dynamic Data Exchange=Dynamischer Datenaustausch). Wenn dieser Dienst beendet wird, stehen keine DDE-Netzwerkfreigaben mehr zur Verfügung. |
| Netzwerkverbindungen – Netman | M/M | SharedAccess | Verwaltet Objekte im Ordner „Netzwerk- und DFÜ-Verbindungen", in dem er sowohl LAN- als auch WAN-Verbindungen anzeigt. |
| NLA (Network Location Awareness) – Nla | M/* | SharedAccess | Sammelt und speichert Netzwerkkonfigurations- und Standortinformationen und benachrichtigt Anwendungen, wenn diese Informationen sich ändern. |
| NT-LM-Sicherheitsdienst – NtLmSsp | M/M | TlntSvr | Bietet Sicherheit für Remote-Prozeduraufrufe (RPC), die andere Transportwege als Named Pipes verwenden. |
| Plug-and-Play – PlugPlay | A/A | Messenger, SCardSrv, TapiSrv, dmserver, dmadmin, AudioSrv | Ermöglicht dem Computer, Hardware-Änderungen zu erkennen und sich mit geringer Benutzerinteraktion darauf einzustellen. Deaktivieren des Dienstes beeinträchtigt die Systemstabilität. |
| QoS-RSVP – RSVP | M/M | – | Bietet Programmen und Systemsteuerungssymbolen, die QoS unterstützen, Installationsfunktionen zur Steuerung von Netzwerksignalen und lokalem Netzwerkverkehr. |
| RAS-Verbindungsverwaltung – RasMan | M/M | SharedAccess, RasAuto | Stellt eine Netzwerkverbindung her. |
| Remote-Prozeduraufruf (RPC) – RpcSs | A/A | beinahe jeder | Endpunktzuordnung und andere verschiedene RPC-Dienste. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
| --- | --- | --- | --- |
| Remote-Registrierung – RemoteRegistry | M/D | – | Ermöglicht Remote-Benutzern, die Registrierungseinstellungen dieses Computers zu ändern. Wenn dieser Dienst beendet wird, kann die Registrierung nur von lokalen Benutzern dieses Rechners verändert werden. |
| Routing und RAS – RemoteAccess | M/M | – | Bietet Routing-Dienste in LAN- und WAN-Netzwerkumgebungen. |
| RPC-Locator – RpcLocator | M/M | – | Verwaltet die Datenbank für den RPC-Namensdienst. |
| Sekundäre Anmeldung – seclogon | A/* | – | Ermöglicht das Starten von Prozessen unter Verwendung alternativer Anmelde-Informationen. Für diese Art der Anmeldung ist dieser Dienst notwendig. |
| Seriennummer der tragbaren Medien – WmdmPmSp | A/D | – | Ermittelt die Seriennummer aller tragbaren Musikabspielgeräte, die an den Computer angeschlossen sind. |
| Server – lanmanserver | A/* | – | Browser Unterstützt Datei-, Drucker- und Named-Piped-Freigabe für diesen Computer über das Netzwerk. Falls dieser Dienst deaktiviert wird, können die Dienste, die ausschließlich von ihm abhängig sind, nicht mehr gestartet werden. |
| Shell-Hardwareerkennung – ShellHW-Detection | A/A | – | - |
| Sicherheitskontenverwaltung – SamSs | A/A | MSDTC | Speichert Sicherheitsinformationen für lokale Benutzerkonten. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Sitzungsmanager für Remote-Desktop-Hilfe – RDSessMgr | M/D | – | Verwaltet und überwacht die Remote-Unterstützung, die beim Beenden des Dienstes nicht mehr verfügbar ist. |
| Smartcard – SCardSrv | M/M | – | Verwaltet den Zugriff auf Smartcards, die von diesem Computer gelesen werden. Wenn dieser Dienst beendet wird, wird dieser Computer keine Smartcards mehr lesen können. |
| Smartcard-Hilfsprogramm – SCardDrv | M/M | – | Ermöglicht die Verwendung herkömmlicher (nicht-Plug-and-Play-fähiger) Smartcard-Leser an diesem Computer. Wenn dieser Dienst beendet wird, wird dieser Computer keine herkömmlichen Smartcard-Leser unterstützen. |
| SSDP-Suchdienst – SSDPSRV | M/D | – | Aktiviert die Ermittlung von UPnP-Geräten auf Heimnetzwerken. |
| Systemereignisbenachrichtigung – SENS | A/A | – | Verfolgt Systemereignisse wie Windows-Anmeldungen sowie Netzwerk- und Stromversorgungsereignisse. Benachrichtigt zudem COM+ Ereignissystembezieher von diesen Ereignissen. |
| Systemwiederherstellung – srservice | A/* | – | Führt Funktionen für die Systemwiederherstellung durch. Deaktivieren Sie „Systemwiederherstellung“ auf der Registerkarte in „Arbeitsplatz / Eigenschaften“, um den Dienst zu beenden. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Taskplaner – Schedule | A/* | – | Ermöglicht einem Benutzer, automatische Vorgänge auf diesem Computer zu konfigurieren und zu planen. Ist der Dienst beendet, werden diese Vorgänge nicht zu den geplanten Zeiten ausgeführt. |
| TCP/IP-NetBIOS-Hilfsprogramm – LmHosts | A/* | – | Ermöglicht die Unterstützung vom NetBIOS-über-TCP/IP-Dienst (NetBT) und die Net-BIOS-Namensauflösung. |
| Telefonie – TapiSrv | M/* | RAS, RasAuto | Bietet Telefonie-API-Unterstützung (TAPI) für Programme, die Telefoniegeräte steuern, sowie IP-basierte Sprachverbindungen am lokalen Computer und über das LAN, auf Servern, die diesen Dienst ebenfalls ausführen. |
| Telnet – TlntSvr | M/D | – | Ermöglicht Remote-Benutzern, sich am Computer anzumelden und Programme auszuführen. Unterstützt verschiedene Telnet-Clients, einschließlich Unix- und Windows-basierten Computern. Bei gestopptem Dienst ist der Remote-Zugriff möglicherweise nicht mehr verfügbar. |
| Terminaldienste – TermService | M/* | FastUser-Switching-Compatibility | Ermöglicht mehreren Benutzern das Herstellen interaktiver Verbindungen mit anderen Computern sowie das Anzeigen von Desktop und Anwendungen auf Remote-Computern. Terminaldienste bilden die Grundlage für Remote-Desktops (einschließlich RD für Administratoren), schnelle Benutzerumschaltung, Remote-Unterstützung und Terminalserver. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| **Dienstname – Kurzname** | **Starttyp Default/ Empfohlen** | **Abhängige Dienste** | **Beschreibung** |
|---|---|---|---|
| Treibererweiterungen für Windows-Verwaltung – Wmi | M/M | – | Unterstützt Systemverwaltungsinformationen von Treibern. |
| Überwachung verteilter Verknüpfungen (Client) – TrkWks | A/* | – | Hält Verknüpfungen für NTFS-Dateien auf einem Computer oder zwischen Computern in einer Netzwerkdomäne aufrecht. |
| Universeller Plug-and-Play-Geräte-Host – upnphost | M/D | – | Ermöglicht es, den Computer als Host für universelle Plug-and-Play-Geräte einzurichten. |
| Unterbrechungsfreie Stromversorgung – UPS | M/M | – | Verwaltet eine an den Computer angeschlossene unterbrechungsfreie Stromversorgung (USV). |
| Upload-Manager – uploadmgr | A/D | – | Verwaltet synchrone und asynchrone Dateiübertragungen zwischen Clients und Servern. Entsprechende Dateiübertragungen werden nicht ausgeführt, wenn Sie diesen Dienst beenden. |
| Verwaltung für automatische RAS-Verbindung – RasAuto | A/* | – | Erstellt eine Verbindung zu einem Remote-Netzwerk, wenn ein Programm eine Remote-DNS- oder -NetBIOS-Adresse referenziert. |
| Verwaltung logischer Datenträger – dmserver | M/M | dmadmin | Erkennt und überwacht neue Festplattenlaufwerke; sendet Festplatteninformationen zur Konfiguration an den Verwaltungsdienst für logische Datenträger. Wenn Sie diesen Dienst beenden, können Status- und Konfigurationsinformationen für Festplatten veralten oder ungültig werden. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| **Dienstname – Kurzname** | **Starttyp Default/ Empfohlen** | **Abhängige Dienste** | **Beschreibung** |
|---|---|---|---|
| Verwaltungsdienst für die Verwaltung logischer Datenträger – dmadmin | M/M | – | Konfiguriert Festplattenlaufwerke und -Volumes. Dieser Dienst wird nur zu Konfigurationszwecken ausgeführt und anschließend beendet. |
| Volume-Schattenkopie – VSS | M/M | – | Verwaltet und implementiert Volume-Schattenkopien, die zu Sicherungs- und anderen Zwecken verwendet werden. Wenn dieser Dienst beendet wird, werden keine Schattenkopien für Sicherungen verfügbar sein, und die Sicherung kann eventuell fehlschlagen. |
| Warndienst – Alerter | M/M | – | Benachrichtigt bestimmte Benutzer und Computer bezüglich administrativer Warnungen. Falls der Dienst beendet wird, können Programme, die administrative Warnungen verwenden, diese nicht mehr empfangen. |
| Web-Client – WebClient | A/D | – | Ermöglicht Windows-basierten Programmen, Internet-basierte Dateien zu erstellen, darauf zuzugreifen und sie zu verändern. |
| Wechselmedien – NtmsSvc | M/M | – | - |
| Windows Audio – AudioSrv | A/A | – | Verwaltet Audio-Geräte für Windows-basierte Programme. Wenn dieser Dienst beendet wird, werden Audio-Geräte und -Effekte nicht korrekt funktionieren. |
| Windows-Installer – MSIServer | M/M | – | Installiert, repariert oder entfernt Software gemäß der in MSI-Dateien enthaltenen Anweisungen. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| Dienstname – Kurzname | Starttyp Default/ Empfohlen | Abhängige Dienste | Beschreibung |
|---|---|---|---|
| Windows-Bilderfassung (WIA) – stisvc | M/M | – | Bietet Bilderfassungsdienste für Scanner und Kameras. |
| Windows-Verwaltung – winmgmt | A/A | – | Verfügt über eine standardmäßige Schnittstelle und ein Objektmodell zum Zugreifen auf Verwaltungsinformationen über das Betriebssystem, Geräte, Anwendungen und Dienste. Die meiste Windows-basierte Software kann nicht ordnungsgemäß ausgeführt werden, falls dieser Dienst beendet wird. |
| Windows-Zeitgeber – W32Time | A/* | – | Verwaltet die Datum- und Uhrzeitsynchronisierung auf allen Clients und Servern im Netzwerk. |
| WMI-Leistungsadapter – WmiApSrv | M/M | – | Bietet Leistungsbibliotheksinformationen der WMI-Hi-Perf-Anbieter. |

Starttyp: A = automatisch, M = manuell, D = deaktiviert, * = Konfiguration nach Bedarf.

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Windows XP Bugreport | a818 | – |
| Test: Windows XP | a602 | – |
| Windows XP Benchmarks | a772 | – |
| Profi-Know-how: Windows boot.ini | a802 | – |
| Windows XP auf Notebooks | a773 | – |

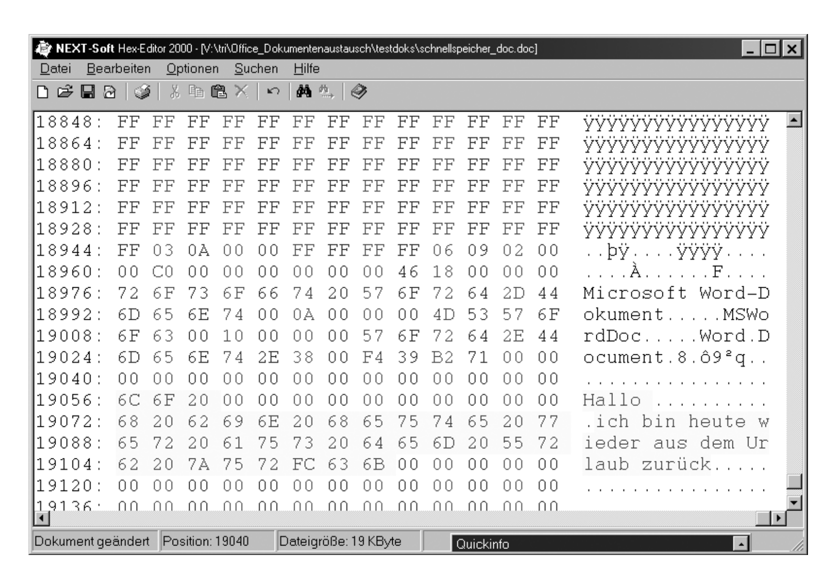
# 3.2 Microsoft-Office-Dateien säubern und signieren

In Office-Dateien steckt mehr als nur der reine Dokumenteninhalt. Wer Daten austauscht, kann so unwissentlich heikle Zusatzinformationen weitergeben. Wir erklären, wie Sie das Risiko minimieren.

Die mit modernen Versionen von Microsofts Office-Suite erstellten Dateien enthalten eine ganze Reihe von Informationen, die sich durch den Benutzer nicht unmittelbar einsehen lassen. Gerade sie verraten aber dem Eingeweihten einiges über den Autor des Dokuments oder das Unternehmen, aus dem es stammt.

So haben etwa gelöschte Textpassagen, die nachträglich wieder sichtbar gemacht wurden, in der Vergangenheit bereits etliche Politiker und Konzerne in Erklärungsnot gebracht. Deshalb sollten Sie Dokumente, die Sie weitergeben werden, prinzipiell von derartigem Ballast bereinigen.

Am einfachsten gelingt die Überwachung der versteckten Informationen noch bei den Meta-Daten, die in den Datei-Eigenschaften stecken. Über die dort gespeicherten Angaben lassen sich beispielsweise statistische Werte wie die Bearbeitungszeit eines Dokuments ermitteln. Welche Datei-Informationen Sie im Einzelnen auslesen und auch verändern können, zeigt unser Beispiel-Makro für Word auf den nächsten Seiten.




**Tückischer Zwischenspeicher:** Bei Copy&Paste landen Daten auch schon mal woanders als vorgesehen, wie hier ein Teil aus einer E-Mail in Word.

Neben den Meta-Daten selbst lässt sich Office-Dateien jedoch noch einiges mehr entlocken. Über einen Hex-Editor findet man beispielsweise nicht nur den Speicherpfad oder den Namen der verwendeten Schriftarten. Es ist ebenso möglich, Informationen aufzuspüren, die als blinde Passagiere über Copy-and-Paste-Aktionen von anderen Anwendungen stammen. Im Folgenden erfahren Sie, wie Sie auch dieses Risiko minimieren.

Nachdem die unerwünschten Informationen aus den Dateien getilgt sind, steht dem Datenaustausch nichts mehr im Wege. Dabei kann man gleichzeitig ein neues Sicherheits-Feature von Office XP einsetzen und durch eine digitale Signatur der nachträglichen Veränderung der Informationen vorbeugen. Auch hierbei gilt es, einige Grundsätze zu berücksichtigen.

## 3.2.1 Meta-Daten

Um die Meta-Daten eines Office-Dokuments einzusehen, genügt es, das Menü „Datei/Eigenschaften“ aufzurufen. Dort finden sich bereits einige sensible Informationen, die man vor neugierigen Blicken schützen sollte. Die Daten lassen sich in folgende Kategorien einteilen:

- Automatisch aktualisierte Datei-Eigenschaften. Hier finden sich statistische Angaben, die durch die Applikation verwaltet werden. Dazu zählen beispielsweise die Größe sowie das Erstell- und Änderungsdatum des Dokuments. Weitaus kritischer ist allerdings der Wert unter „Bearbeitungszeit“. Diese Angabe kann ein Unternehmen zur Leistungskontrolle seiner Mitarbeiter heranziehen, ohne dass diese es bemerken.
- Vorbelegte Datei-Eigenschaften. Beim Anlegen eines neuen Dokuments füllt die jeweilige Office-Applikation bereits bestimmte Felder wie Autor und Firma aus. Die erforderlichen Informationen entnimmt die Software den Angaben, die der Anwender bei der Installation von Office oder Windows gemacht hat. Als Dokumententitel trägt die Applikation beim ersten Speichern die 126 Zeichen am Anfang der Datei ein – vorausgesetzt, der Anwender gibt nicht selbst explizit einen Titel an.
- Benutzerdefinierte Datei-Eigenschaften. Hierunter fallen Angaben, denen der Anwender Text, ein Datum, eine Zahl oder den Wert „Ja“ oder „Nein“ zuordnen kann. Es besteht sowohl die Möglichkeit, aus einer Liste mit vordefinierten Namen zu wählen als auch eigene Felder hinzuzufügen. Darüber hinaus lassen sich auch benutzerdefinierte Datei-Eigenschaften mit bestimmten Elementen einer Datei verknüpfen – beispielsweise einer benannten Zelle in Excel oder einer Textmarke in Word.

Auf den folgenden Seiten erfahren Sie, auf welche dieser Eigenschaften Sie schreibend zugreifen können und was es dabei zu beachten gilt.

### 3.2.2 Zugriff auf Meta-Daten

Die Felder, die man über den Aufruf von „Datei/Eigenschaften“ erreicht, lassen sich auch über ein Makro ansprechen. Die Idee, für deren Säuberung den Makro-Recorder einzusetzen, liegt zwar nahe, führt aber nicht zum gewünschten Ergebnis: Das Utility zeichnet nichts auf.

Nutzer von Office XP können die persönlichen Informationen jedoch auch unter „Extras/Optionen/Sicherheit“ mit einem Klick entfernen. Allen anderen bleibt nichts anderes übrig, als den erforderlichen Code selbst einzugeben.

Der Zugriff auf die Dokumenteigenschaften gelingt über die BuiltInDocument-Properties. Mittels Aufruf der VBA-Funktion Activedocument.BuiltInDocument Properties.Count in Word erfährt man, dass es insgesamt 30 dieser Eigenschaften gibt. Eine Durchsicht ergibt, dass acht davon vertrauliche Informationen enthalten können und sich gegebenenfalls ändern lassen:

| Relevante Dokumenteigenschaften in Word 2000/XP | | |
|---|---|---|
| **ID** | **Word-Konstante** | **Deutsches Dialogfeld** |
| 1 | wdPropertyTitle | Titel |
| 2 | wdPropertySubject | Thema |
| 3 | wdPropertyAuthor | Autor |
| 4 | wdPropertyKeywords | Stichwörter |
| 5 | wdPropertyComments | Kommentar |
| 18 | wdPropertyCategory | Kategorie |
| 20 | wdPropertyManager | Manager |
| 21 | wdPropertyCompany | Firma |

Über die jeweilige VBA-Hilfe, Stichpunkt „BuiltInDocumentProperties“, erhält man die Konstanten der anderen Office-Programme.

Die ID ist eine von Microsoft vergebene Zahl, die alternativ zur Word-Konstante den Zugriff auf Felder ermöglicht. Das Feld „Autor“ etwa lässt sich sowohl über ActiveDocument.BuiltinDocumentProperties(wdPropertyAuthor) als auch über ActiveDocument.BuiltinDocumentProperties(3) ansprechen.

### 3.2.3 Überwachung ausschalten

Einige Datei-Eigenschaften lassen sich zwar auslesen, aber weder manuell noch per Makro verändern. Dazu gehören statistische Angaben wie das Erstell- und Änderungsdatum, die Anzahl der Wörter sowie die Bearbeitungszeit.




**Lesen ja, schreiben nein:** Die statistischen Auswertungen lassen sich nicht ändern.

Immerhin kann man jedoch unschwer feststellen, ob die Bearbeitungszeit überhaupt mitprotokolliert wird: Darüber entscheidet der Registry-Schlüssel „NoTrack“, der sich unter HKEY_CURRENT_USER findet:

| Registry-Pfade für NoTrack in Office 2000/XP | |
|---|---|
| **Office-Version** | **Registry-Schlüssel** |
| Office 2000 | HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Common\General\NoTrack |
| Office XP | HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Common\General\NoTrack |

Ist NoTrack gleich 1, wird die Bearbeitungszeit nicht protokolliert. Das gilt auch, wenn der Schlüssel fehlt.

Diese Überwachungsfunktion ist aus rechtlichen Gründen in deutschen Office-Versionen standardmäßig deaktiviert. Nach dem Betriebsverfassungsgesetz unterliegen Maßnahmen zur Zeiterfassung in deutschen Unternehmen der Mitbestimmung durch den Betriebsrat.

### 3.2.4 Beispielmakro für Word

Das folgende VBA-Makro läuft sowohl unter Word 2000 als auch unter Word XP. Es prüft zunächst in einer If-Abfrage die vorliegende Version der Textverarbeitung. Abhängig davon weist die Prozedur dann den Datei-Eigenschaften Titel, Thema, Autor, Manager, Firma, Kategorie, Stichwörter und Kommentar einen Leer-String zu.

Ob die Bearbeitungszeit im Dokument aufgezeichnet wird, verrät der Registry-Wert von „NoTrack“. Beträgt er Null (Protokoll eingeschaltet), dann setzen wir ihn auf Eins (Protokoll deaktiviert).

```
Sub ClearDocProps()

Dim strPropVal, strVersion, regpath As String
strPropVal = ""
strVersion = Application.Version

if strVersion = "9.0" then
 regpath = "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\
Common\General"
elseif strVersion = "10.0" then
 regpath = "HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\
Common\General"
end if

If strVersion = "9.0" Or strVersion = "10.0" Then
  With ActiveDocument
 .BuiltInDocumentProperties(wdPropertyTitle) = strPropVal
 .BuiltInDocumentProperties(wdPropertySubject) = strPropVal
 .BuiltInDocumentProperties(wdPropertyAuthor) = strPropVal
 .BuiltInDocumentProperties(wdPropertyManager) = strPropVal
 .BuiltInDocumentProperties(wdPropertyCompany) = strPropVal
 .BuiltInDocumentProperties(wdPropertyCategory) = strPropVal
 .BuiltInDocumentProperties(wdPropertyKeywords) = strPropVal
 .BuiltInDocumentProperties(wdPropertyComments) = strPropVal
  End With
Else
  MsgBox "Das Makro läuft nur mit Word 2000 oder Word XP."
  End
End If

If System.PrivateProfileString("", regpath, "NoTrack") = 0
Then
 System.PrivateProfileString("", regpath, "NoTrack") = 1
End If

End Sub
```

### 3.2.5 Versteckte Informationen

Abgesehen von den Meta-Daten können sich in Office-Dateien noch weitere Informationen verbergen, die Unbefugte brennend interessieren dürften. Diese sensiblen Daten sieht man allerdings erst dann, wenn man das Dokument mit einem Text-Editor öffnet.

Neben internen Verwaltungsangaben wie Speicherpfad oder verwendeter Dokumentvorlage tauchen mitunter Daten auf, die man während einer Arbeitssitzung per Copy-and-Paste zwischen anderen Applikationen ausgetauscht hat. Wir untersuchen mit Office 2000 und XP, ob es Umstände gibt, die dieses Verhalten begünstigen. Als Hauptverdächtigen knöpfen wir uns zunächst Word vor.

Nicht ohne Grund, denn Microsoft selbst rät in einem Artikel im Hilfecenter, Funktionen der Textverarbeitung wie die Schnellspeicherung zu deaktivieren. Ansonsten, so der Hersteller, liefe der Anwender Gefahr, dass Informationen gespeichert würden, die er bereits gelöscht hat.

Das können wir bestätigen, da Word bei aktiver Schnellspeicherung die Änderungen einfach ans Ende des Dokuments anhängt. Das bläht unnötigerweise die Größe der Datei auf. Nicht erklären können wir uns hingegen, weshalb plötzlich eine Zeile aus einer Outlook-Mail im Dokument auftaucht. Diese hatten wir zuvor in den Zwischenspeicher kopiert, um sie in einer anderen Nachricht einzufügen.

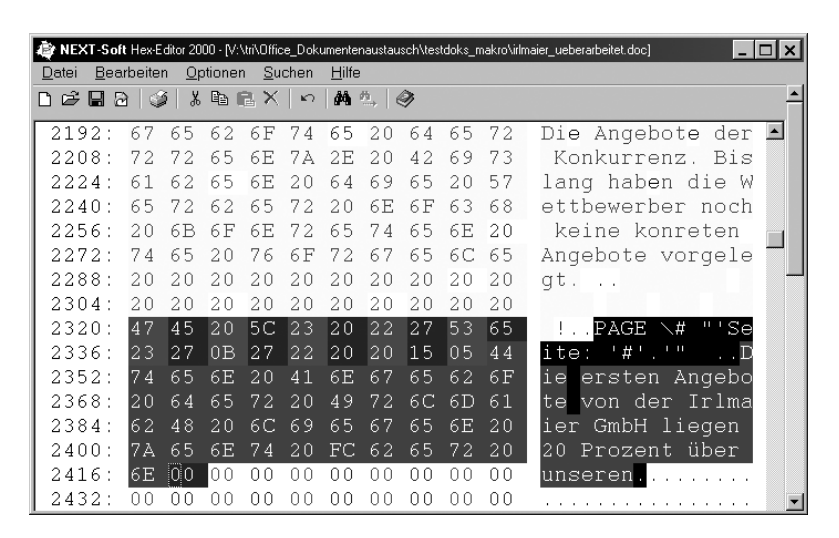
Hier drängt sich der Verdacht auf, dass pauschal RAM-Bereiche angesprochen werden. Erst ein „Speichern unter“ bereinigt die Sache wieder. In unseren Tests treffen wir in keiner der anderen Office-Anwendungen auf den Fehler, er bleibt auf Word beschränkt.

### 3.2.6 Bearbeitungshistorie mit Macken

Word erleichtert das gemeinsame Arbeiten an Texten durch die Überarbeiten-Funktion. Mit einem Klick geht ein Text an die Kollegen im Team, die den Text, die Präsentation oder die Tabelle überarbeiten. Anschließend schicken sie die korrigierten Dokumente wieder zurück. Änderungen des jeweiligen Bearbeiters samt Kommentaren lassen sich leicht im Dokument nachvollziehen. Über „Extras/Änderungen“ erhält man so Einblick in die Entstehungsgeschichte von Dateien.

Sind alle Nachbesserungen angebracht, können die Versionen zu einer gemeinsamen Fassung zusammengefügt werden. Damit sollten gleichzeitig auch die Korrekturvorschläge verschwinden – was nach unseren Erfahrungen jedoch nur eingeschränkt stimmt.

Denn die aktivierte Schnellspeicherung sorgt dafür, dass die Bearbeitungshistorie mit einem Hex-Editor weiterhin zugänglich ist. Die verräterischen Spuren verschwinden bei unseren Versuchen erst, als wir die Schnellspeicherung abschalten und das Dokument mit der Option „Speichern unter“ ablegen.




**Verräterische Anmerkung:** Die Konkurrenz dürfte sich über solche brisanten Firmeninformationen freuen.

Was einerseits den Workflow in Unternehmen vereinfacht, kann andererseits im ungünstigen Fall zum Politikum werden. Ein bekanntes Beispiel: Im Februar 2002 hatte sich ein Journalist die Kurzfassung der Metrorapid-Machbarkeitsstudie als Word-Datei von der Webseite des nordrhein-westfälischen Verkehrsministeriums heruntergeladen.

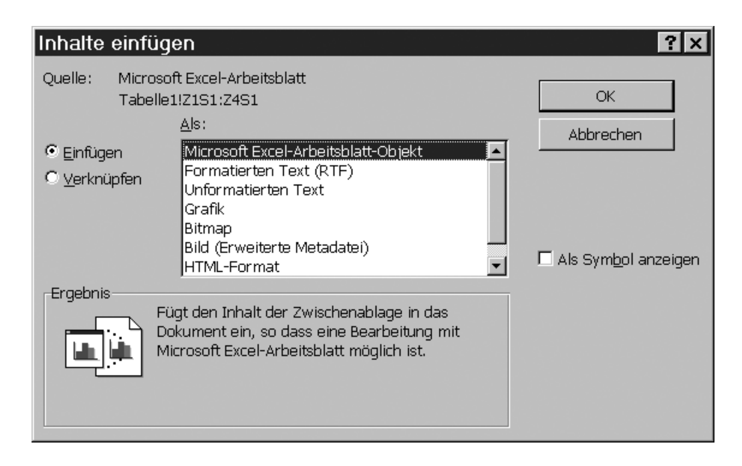
Über die Funktion „Änderungen verfolgen“ stellte er fest, dass die Gutachter wesentliche Textpassagen kurz vor der Veröffentlichung gelöscht hatten. Schon kurze Zeit später meldete die „Süddeutsche Zeitung“, die Machbarkeitsstudie sei schöngerechnet worden.

## 3.2.7 Gelinkt mit OLE

Aus Microsofts Office-Suite fällt uns neben der Textverarbeitung auch die Tabellenkalkulation unangenehm auf. Immer dann, wenn der Anwender Daten aus Excel 2000 per OLE in andere Applikationen übernimmt, kann mehr mitkopiert werden als vorgesehen. Wer etwa seine Outlook-Mails im RTF-Format schreibt, sollte aufpassen, wenn er einige Zellen aus Excel als Objekt in die Nachricht einfügt.

Denn der Empfänger sieht mit einem Doppelklick nicht nur die ausgewählten Informationen, sondern bekommt das komplette Arbeitsblatt zu Gesicht. Auf diese Weise kann eine angeforderte Liste mit Mitarbeiternamen zusätzliche Angaben – wie etwa private Telefonnummern oder Beurteilungen – preisgeben, ohne dass der Absender sich dessen bewusst ist.

Die einfachste Abhilfe besteht darin, auf ein anderes Nachrichtenformat als RTF auszuweichen. Aber auch wer die Daten über „Bearbeiten/Inhalte einfügen“ kopiert und dabei nicht die Option „Microsoft Excel Worksheet“ anwählt, ist auf der sicheren Seite.



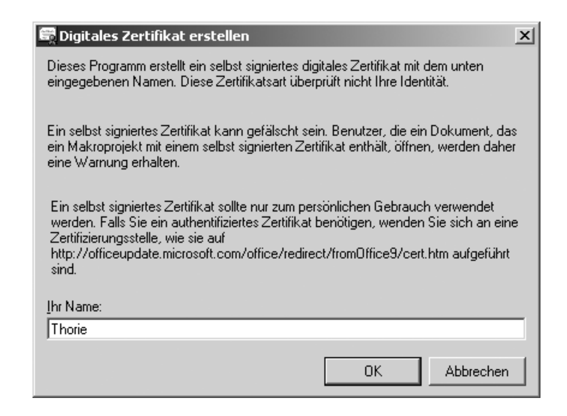

**Gefahrenquelle OLE:** Beim Datenaustausch mit Microsofts Tabellenkalkulation sollte man auf ein Excel-Objekt verzichten.

Ähnlich unangenehme Effekte können nach unserer Erfahrung ebenfalls bei der Datenübernahme von Excel in PowerPoint oder Word auftreten. Auch dabei besteht die Gefahr, dass nicht nur die markierten Zellen in der Präsentation oder in dem Dokument landen, sondern stattdessen das vollständige Arbeitsblatt. Verzichtet man hingegen darauf, die Informationen als OLE-Objekt einzufügen, tritt der Fehler nicht auf.

Stammt eine der am Datenaustausch beteiligten Applikationen aus Office XP, können wir das beschriebene Fehlverhalten nicht feststellen. In den zugehörigen Knowledgebase-Artikeln (http://support.microsoft.com) Q196231 und Q232866 spricht Microsoft übrigens keineswegs von einem Bug, sondern beschreibt das Verhalten euphemistisch als „Problem“.

## 3.2.8 Digitale Signaturen mit Office

Elektronische Daten können leicht gefälscht werden, ohne Spuren zu hinterlassen. Genau das soll die digitale Signatur verhindern. Sie sorgt einerseits dafür, dass sich der Empfänger der Information darauf verlassen kann, dass die Nachricht tatsächlich vom angegebenen Absender stammt. Außerdem garantiert die Signatur, dass kein Unberechtigter die Nachricht nachträglich manipuliert hat.

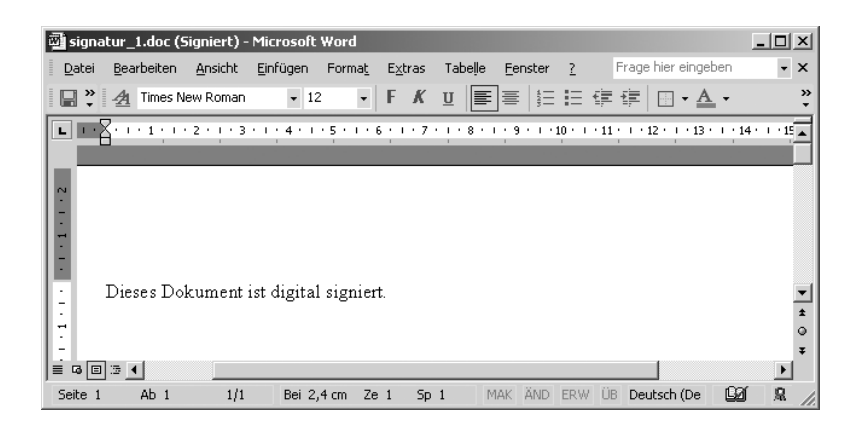



**Selbst zertifiziert:** Mit dem in Office enthaltenen Tool Selfcert.exe kann sich jeder selbst eine Unbedenklichkeitserklärung ausstellen.

Mit Office XP lassen sich nicht nur wie in der Vorgängerversion Makros digital signieren. Microsofts neueste Büro-Suite versieht erstmals ganze Dokumente in Word, Excel und PowerPoint mit einer elektronischen Unterschrift.

Für die Authentizität der verwendeten Signatur wiederum bürgen so genannte digitale Zertifikate. Theoretisch kann jeder Anwender mit Hilfe entsprechender Tools sein eigenes Zertifikat ausstellen. Dazu lässt sich etwa das in Office enthaltene Programm Selfcert.exe nutzen.

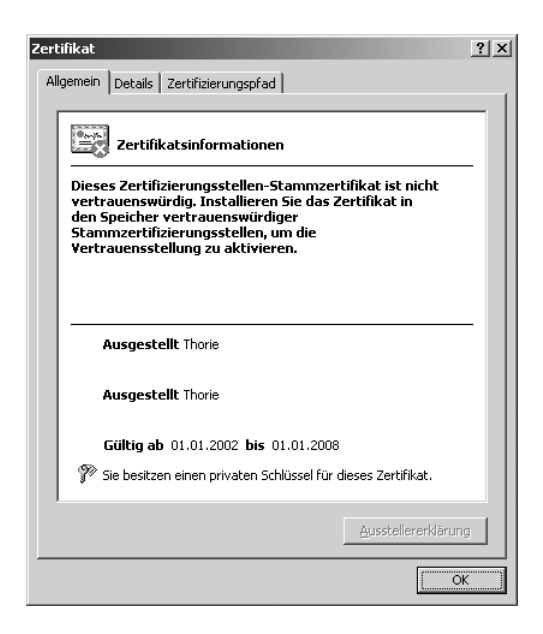
Doch ein solches „Gütesiegel“ wirkt genauso vertrauenerweckend wie ein vom Inhaber selbst ausgestellter Personalausweis. Daher sollte man das Ausstellen des digitalen Zertifikats nicht selbst erledigen, sondern es stattdessen einem „vertrauenswürdigen Dritten“ überlassen.




**Dezente Zeichen:** Ob ein Dokument digital signiert ist, sehen Sie nur an Titel- und Statuszeile.

Diese so genannten Trust Center wie VeriSign TC TrustCenter oder TeleSec stellen Testzertifikate meist kostenlos aus. Die durchgeführte Überprüfung für solche Klasse-1-Zertifikate beschränkt sich allerdings in der Regel auf die angegebene E-Mail-Adresse. Zumindest kann man sich auf diese Weise mit der doch recht komplexen Materie etwas vertraut machen.

Egal ob Testzertifikat oder nicht: Um die so erhaltenen elektronischen Bescheinigungen in Office zu verwenden, muss der Anwender sie über den Internet Explorer (IE) installieren. Dazu verschickt der Aussteller eine URL oder eine Datei. Erstere ruft man einfach im Browser auf, Letzere importiert man über die IE-Internet-Optionen. Danach lassen sich dann Word-, Excel- und PowerPoint-Dateien digital signieren.

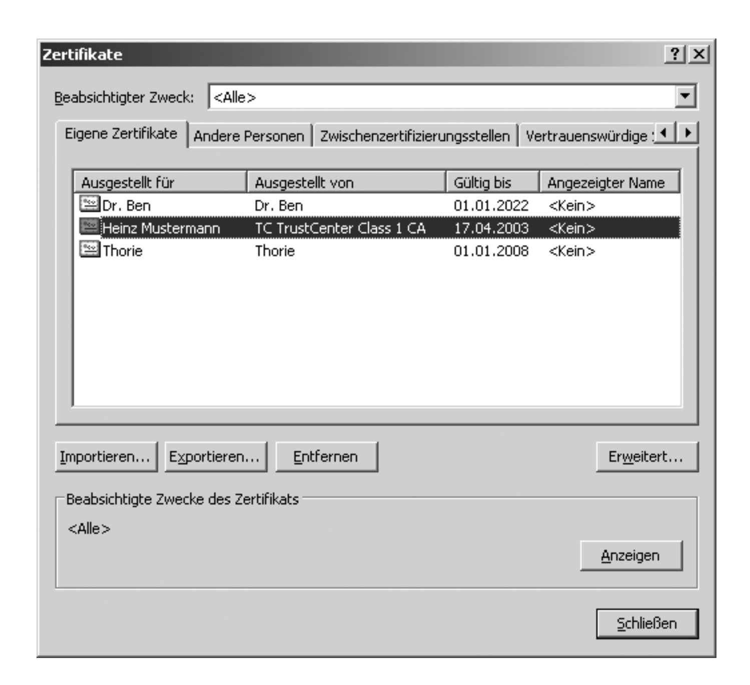



**Durchgefallen:** Mit Selfcert.exe erstellte Nachweise werden als nicht vertrauenswürdig eingestuft.

Die entsprechende Option findet sich in allen drei Applikationen unter dem Menüpunkt „Extras/Optionen/Sicherheit/Digitale Signaturen“. Sinnvollerweise sollte das Signieren der letzte Bearbeitungsschritt sein, den Sie an einem Dokument durchführen: Eine Änderung am Inhalt entfernt die bisherigen Signaturen.

### 3.2.9 Überprüfen des Zertifikats

Ob Ihnen jemand eine signierte Datei geschickt hat, sehen Sie beim Öffnen in Office XP am Zusatz „(Signiert)“ neben dem Dokumentnamen in der Titelzeile. Außerdem erscheint rechts unten in der Statuszeile ein rot-gelbes Siegel als Icon.




**Gestatten, Heinz Mustermann:** Nicht nur das Trust Center muss vertrauenswürdig sein, auch der Inhaber eines Zertifikats.

Ein Doppelklick auf das rot-gelbe Siegel-Icon in der rechten unteren Ecke des Fensters fördert bereits erste Informationen wie den Namen des Absenders und das Ausstellungsdatum des Zertifikats zu Tage.

Entscheidend für die Gültigkeit des Zertifikats sind aber nicht zuletzt auch die Details, die Sie über die Schaltfläche „Zertifikat anzeigen“ erhalten. Speziell anhand des Eintrags im Feld „Ausgestellt von“ sollten Sie gewissenhaft entscheiden, ob Sie dem Trust Center, der Organisation oder der Person, die das Zertifikat ausgestellt hat, vertrauen.

Besondere Vorsicht ist stets dann angebracht, wenn sich im Kommentarabschnitt folgender Hinweis findet: „Das Zertifikat dieser Zertifizierungsstelle ist nicht vertrauenswürdig. Damit es als vertrauenswürdig eingestuft wird, installieren Sie dieses Zertifikat im Bereich vertrauenswürdiger Zertifizierungsstellen.“

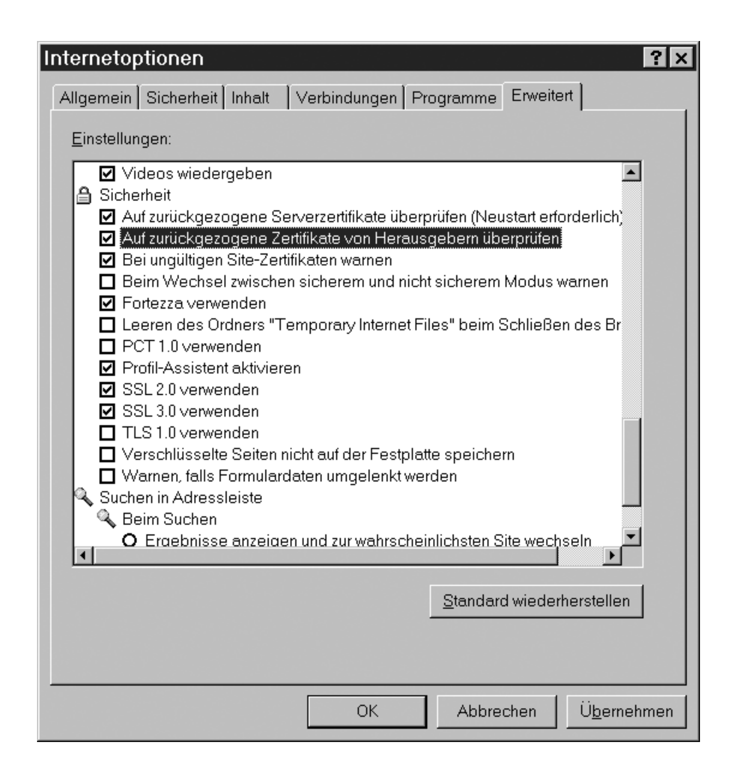
Diese Formulierung kann beispielsweise darauf hindeuten, dass sich hier jemand mit dem Tool Selfcert.exe selbst eine Unbedenklichkeitserklärung ausgestellt hat. Auch Kommentare wie „Demo“, „Test“ oder „Beispiel“ lassen besondere Wachsamkeit dem Zertifikat gegenüber als ratsam erscheinen.

## 3.2.10 Vertrauen auf Zeit

Dass Sie dem Herausgeber eines Zertifikats vertrauen, stellt nur den ersten Schritt bei der Überprüfung dar. Gleiches muss aber auch für die Person oder Organisation gelten, für die der Nachweis ausgestellt wurde. Oder würden Sie einem Ihnen unbekannten Heinz Mustermann vertrauen, nur weil ein bekanntes Trust Center sich für seine Identität verbürgt?

Außerdem gelten Zertifikate nur für einen bestimmten Zeitraum, danach verfallen sie. Doch auch vor Ablauf dieses Verfallsdatums kann der Aussteller ein Zertifikat zurückziehen: etwa dann, wenn Unregelmäßigkeiten auftreten.

Um stets auf dem Laufenden zu sein, kann man den Internet Explorer anweisen, die Liste zurückgezogener Zertifikate laufend auf dem aktuellen Stand zu halten. Dazu muss man über „Extras/Internetoptionen/Erweitert“ im Sicherheitsbereich den Punkt „Auf zurückgezogene Zertifikate von Herausgebern überprüfen“ aktivieren – was standardmäßig nicht der Fall ist.




**Vertrauen ist gut, Kontrolle ist besser:** Die Liste zurückgezogener Zertifikate hält der Internet Explorer nur auf ausdrücklichen Wunsch aktuell.

### 3.2.11 Fazit

Wer mit Microsofts Office-Paket Daten sicher austauschen will, muss einige Dinge beachten. Jede der Applikationen aus der Büro-Suite speichert in den Dateien Meta-Daten. Dazu gehören der Name des Autors und der Firma. Aber auch die Protokollfunktion, mit der sich feststellen lässt, wie lange jemand an einem Dokument gearbeitet hat.

Diese Angaben können zwar nützlich sein, etwa für Freiberufler, die einen Überblick über ihren zeitlichen Aufwand benötigen. Doch vor der Weitergabe von Dateien sollte man sensible Informationen entfernen. Unser Beispiel-Makro für Word 2000/XP zeigt, wie es funktioniert.

Weitere Angaben, die sich in den Tiefen einer Office-Datei verstecken, lassen sich über einen Hex-Editor zu Tage fördern. Auf wirklich Heikles in Form ganzer Copy-and-Paste-Puffer kann man beispielsweise in Word-Dateien treffen – sofern die Schnellspeicherfunktion der Textverarbeitung aktiv ist. Unter derselben Voraussetzung verrät die Überarbeiten-Funktion die Entstehungsgeschichte von Dokumenten, inklusive aller Kommentare.

Aber auch die Tabellenkalkulation verrät mehr, als sie dürfte. So sollte man darauf verzichten, markierte Zellen einer Datei unter Excel 2000 als OLE-Objekt in andere MS-Office-Applikationen einzufügen. Ein Doppelklick beschert dem Empfänger einen Blick auf das gesamte Arbeitsblatt – der Begriff pars pro toto erhält so eine ganz neue Dimension.

Microsofts Büro-Suite enthält aber nicht nur Gefahrengut. So lassen sich mit Office XP erstmals auch Dokumente aus Word, Excel und PowerPoint heraus digital signieren. Damit bekommt der Anwender ein probates Mittel an die Hand, um ausgetauschte Dokumente auf Authentizität zu prüfen.

Thomas Rieske

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Office-2000-Bugreport | a302 | – |
| Office-XP-Bugreport | a752 | – |
| Test: Office XP Final | a624 | – |
| Elektronisch unterschreiben | a402 | – |

# 3.3 Computerviren-Grundlagen

Stellen Sie sich vor, Sie schalten Ihren Rechner ein – und er bootet nicht. Die Ursache dafür könnte beispielsweise ein Bootvirus wie Parity.B sein. Dieser Uraltvirus aus dem Jahr 1992 ist durchaus in der Lage, ein System mit Windows NT und NTFS-Dateisystem völlig lahm zu legen.

Als noch unangenehmer können sich Würmer erweisen, besonders solche, die gezielt nach nicht gestopften Windows-Sicherheitslücken Ausschau halten. Klez und Bugbear haben gezeigt, dass vor allem viele Server offen wie Scheunentore sind. Offenbar kommen die Admins mit dem Einspielen von Patches nicht mehr nach – oder sie testen zunächst an einigen wenigen Systemen, ob der Microsoft-Fix selbst nicht unangenehme Nebenwirkungen mit sich bringt. Aber auch Linux ist nicht mehr so sicher, wie das massive Auftreten von Slapper gezeigt hat, der eine Vielzahl von Apache-Webservern infiziert hat.

Trotz aller modernen Angriffstaktiken, seien sie technischer oder psychologischer Natur, ist der Anwender den ungebetenen Gästen nicht machtlos ausgeliefert. Wir zeigen, wie die verschiedenen Arten von Malware funktionieren und wie man sich gegen sie wappnen kann.

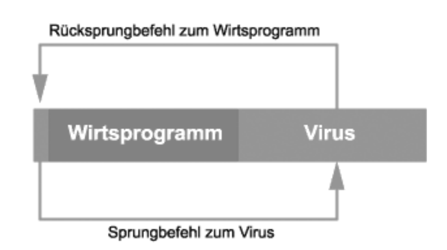
## 3.3.1 Aufbau von Viren

Viren sind Programme, die sich selbst kopieren und auf diese Weise verbreiten. Dazu benötigen sie einen Wirt, dessen Code sie manipulieren, damit sie regelmäßig gestartet werden, etwa um die Schadensfunktion auszuführen. Der interne Aufbau eines Computervirus besteht in der Regel aus drei Modulen: Infektionsroutine, Kopierroutine sowie Statusroutine.

Der Infektorteil ist der elementarste Bestandteil eines Computervirus. Er spürt ein geeignetes Wirtsprogramm auf und infiziert es. Außerdem beinhaltet dieses Modul die Aktivierungsbedingung (Trigger) und die Schadensroutine (Payload). Um eine frühzeitige Entdeckung des Virus zu vermeiden, versucht der Infektor auch, alle verdächtigen Aktivitäten zu tarnen. Dazu kann beispielsweise auch gehören, aktive Antiviren-Programme zu stoppen.

Die Kopierroutine überträgt den viralen Code in andere Wirtsdateien. Dieser Programmteil kann zusätzlich das Zwischenspeichern von Daten übernehmen, die der Virus verlagert hat, etwa aus dem Bootsektor oder MBR.

Das dritte Modul, die so genannte Statusroutine, dient zur Kontrolle und soll Mehrfachinfektionen verhindern. In der Regel setzt der Statusteil ein bestimmtes Bit als Flag in der Wirtsdatei, an dem der Virus erkennt, ob er die Datei bereits infiziert hat oder nicht.




**Umleitung:** Der Virus platziert einen Sprungbefehl am Anfang des Wirtsprogramms, so dass er die Kontrolle über den weiteren Ablauf übernimmt.

Bei einer Infektion klinkt sich ein Virus in den Code eines Wirtsprogramms ein und platziert an dessen Beginn einen Sprungbefehl. Dieser ruft beim Start der verseuchten Datei den angehängten Virus auf. Der kann nun seine Instruktionen ausführen und übergibt am Schluss die Kontrolle wieder an das ursprüngliche Programm, das ganz normal weiterarbeitet. Daher bemerkt der Anwender im Allgemeinen nichts von diesem Vorgang.

### 3.3.2 Wie kommt der Virus auf den PC?

Wie kommt ein Virus auf Ihren PC? Zunächst bekommen Sie von irgendwoher – von einer Diskette, einer CD oder als Download aus dem Internet – eine Programmdatei oder ein makrofähiges Dokument, das einen Virus enthält.

Wenn Sie das Programm starten oder das Dokument öffnen, wird der Virus aktiv. Er nistet sich als Erstes so im System ein, dass er von nun an bei jedem PC-Start automatisch aktiv wird – Makroviren beispielsweise in der Datei normal.dot, die WinWord bei jedem Start lädt. Dateiviren befallen eine Programmdatei, die Windows bei jedem Systemstart automatisch ausführt. Bootviren werden ganz automatisch noch während des PC-Startvorgangs aktiviert.

Entscheidend für die Virenabwehr ist es, dieses Einnisten im System zu verhindern. Solange der Virus nicht gestartet ist, kann er auch keinen Schaden anrichten. Wie schaffen es nun Viren, das erste Mal aktiv zu werden?

### 3.3.3 Infektionswege

Bei Makroviren für Microsoft-Programme ist die Geschichte einfach: Die Makros sind Teil des Office-Dokuments. Bestimmte Makros wie AutoOpen führen Excel, Word oder Access automatisch aus, wenn Sie das Dokument öffnen. Und der Makrovirus klinkt sich – im einfachsten Fall – in dieses AutoOpen-Makro ein.

Bootviren werden bei einem Systemstart nur dann aktiv, wenn eine verseuchte Diskette zufällig im Laufwerk steckt. Versucht der PC, von dieser Diskette zu booten, aktiviert er den Virus. Der einfachste Schutz: Schalten Sie im BIOS das Booten von Diskette aus. Im Zweifelsfall lässt es sich leicht wieder einschalten. Multipartite-Viren und Dropper unterlaufen diese simple Abhilfe: Multipartite-

Viren nutzen mehrere der bisher bekannten Techniken zugleich, sind beispielsweise sowohl Datei- als auch Bootviren. Dropper sind einfache Programme, die beim Start einen Bootvirus in den Systembereich der Festplatte oder Diskette schreiben. Es gibt sogar Makroviren, die als Schadensroutine einen klassischen Bootvirus installieren.

Bei Dateiviren ist die Sache ziemlich klar: Sie bekommen von irgendwoher eine infizierte Programmdatei und starten sie. Damit wird zuerst der Virus aktiv und infiziert weitere Dateien oder nistet sich im System ein. Anschließend startet der Virus das Originalprogramm, so dass Sie von seiner Anwesenheit gar nichts bemerken – vorerst zumindest.

### 3.3.4 In freier Wildbahn

Von den über 20.000 verschiedenen Viren spielt nur ein Bruchteil auf der öffentlichen Bühne, also den PCs der Anwender, eine Rolle.

Seit 1993 sammelt der Amerikaner Joe Wells aus aller Welt Berichte über Virenbefall und stellt sie monatlich in seiner WildList (www.wildlist.org) zusammen. Etwa hundert verschiedene Viren machen 99 Prozent der Infektionen aus. Es fällt auf, dass die Verbreitung des Internet dafür sorgt, dass neue Viren schneller Einzug in die WildList halten und auch wieder daraus verschwinden.

So ist die Zahl der Makroviren in der WildList für Dezember 2002 massiv zurückgegangen. Die Dateiviren haben durch die Verbreitung als E-Mail-Anhang neuen Aufwind erhalten. Sie sind jedoch meist leicht zu finden und zu entfernen. Ein langes Leben haben dagegen Bootviren, die sich auf Disketten jahrelang unbemerkt verstecken können.

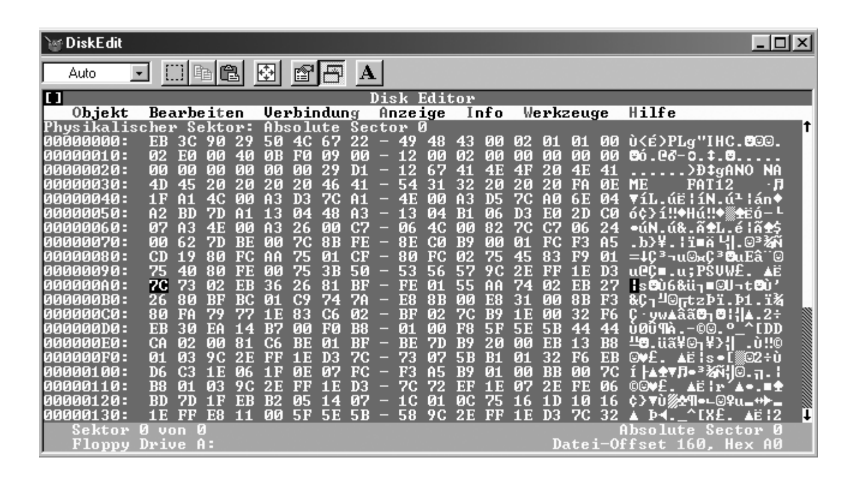
| J. Wells WildList für Dezember 2002, sortiert nach Häufigkeit | | |
|---|---|---|
| **Name** | **Typ** | **Alternative Namen** |
| W32/Klez.H-mm | Datei | – |
| W32/SirCam.A-mm | Datei | – |
| W32/BadTrans.B-mm | Datei | – |
| W32/Magistr.A-mm | Datei | – |
| W32/Nimda.A-mm | Datei | – |
| W32/Magistr.B-mm | Datei | – |
| W32/Klez.E-mm | Datei | – |
| W32/BugBear-mm | Datei | – |
| W32/Hybris.B-mm | Datei | Hybris.23040-mm |
| W32/Goner.A-mm | Datei | – |

| W32/Nimda.E-mm | Datei | – |
|---|---|---|
| W32/Funlove. | Datei | 4099 |
| W32/Elkern.C | Datei | WQK.C |
| W32/MTX-m | Datei | Apology; Matrix |
| W32/Aliz.A-mm | Datei | – |
| W32/Gibe.A-mm | Datei | – |
| W32/Yaha.G-mm | Datei | Lentin.F |
| W95/Spaces.1445 | Datei | Busm.1445 |
| JS/Kak.A-m | Script | – |
| VBS/Haptime.A-mm | Script | Help |
| W32/Braid.A-mm | Datei | – |
| W32/MyParty.A-mm | Datei | – |
| W95/CIH.1003 | Datei | CIH.A; Spacefiller |
| VBS/LoveLetter.A-mm | Script | BugFix; I-Worm |
| W32/FBound.C-mm | Datei | – |
| W32/Hybris.D-mm | Datei | Hybris.25088-mm |
| VBS/Redlof.A-m | Script | – |
| W32/BadTrans.A-mm | Datei | 13312 |
| VBS/LoveLetter.AS-mm | Script | Plan.A |
| W32/Yaha.E-mm | Datei | Lentin.D |
| W97M/Marker.C | Makro | Spooky.C |

### 3.3.5 Boot- und Dateiviren

Mit einem Bootvirus fing alles an: 1986 verbreitete sich Pakistani Brain innerhalb eines Jahres rund um die Welt, obwohl der Virus nur Disketten und keine Festplatten infizierte. Bootviren funktionieren ähnlich wie ein Betriebssystem: Beim Start eines PCs führt das eingebaute BIOS-Programm eine kleine Startroutine von der Festplatte aus. Sie ist im MBR am Anfang der Festplatte gespeichert. Dieses Startprogramm ruft den Start-Code von Windows oder eines anderen Betriebssystems im Bootsektor der aktiven Partition auf.

Auch jede Diskette hat einen Bootsektor. Dort und/oder im MBR ersetzen Bootviren den Start-Code. So wird der Schädling vor allen anderen Programmen aktiv und kann jede eingelegte Diskette infizieren. Danach aktiviert er den normalen Boot-Code des Betriebssystems – der Anwender merkt davon nichts.




**Spurensuche:** Der Bootsektor einer mit Parity. B infizierten Diskette im Norton DiskEditor.

Der Infektionsweg für einen Bootvirus ist klar: Beim Einschalten des PCs liegt eine Diskette im Laufwerk, und der PC versucht, davon zu booten. Weil ein Bootvirus keine Datei zur Verbreitung benötigt, kann auch eine ganz „leere“ Diskette einen Bootvirus enthalten. Da Bootviren auf diese Weise lange Zeit unbemerkt bleiben, gehören Sie zu den hartnäckigsten Vertretern ihrer Art.

Ein beliebiges Programm – ein so genannter Dropper – kann beim Start ebenfalls einen Bootvirus auf die Festplatte oder Diskette kopieren. Selbst einige Makroviren gehen so vor. Darüber hinaus gibt es so genannte Multipartite-Viren, die die Eigenschaften von Boot- und Dateiviren vereinen.

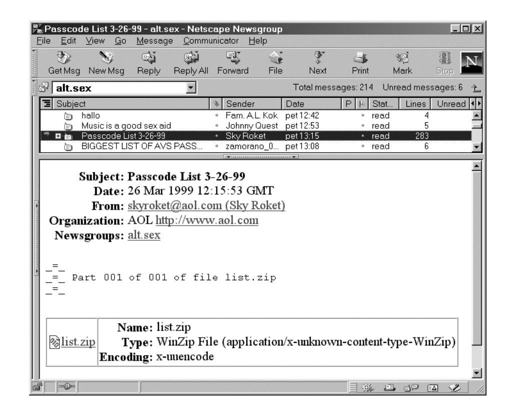
Dateiviren attackieren ausführbare Programmdateien, in die sie ihren eigenen Code kopieren. Wenn das manipulierte Programm gestartet wird, aktiviert das zunächst den Virus, der nun weitere Programme infizieren oder seine Schadensfunktion ausüben kann. Dann lädt er das Originalprogramm.

## 3.3.6 Angriff über NTFS-Streams

Anfang September 2000 sahen sich Windows-NT/2000-User einer völlig neuen Virengattung ausgesetzt, die alle bis dato implementierten Abwehrmaßnamen unterlief. W2K.Stream, so der Name des Schädlings, nutzt ein spezielles Feature des NTFS-Filesystems: die Aufteilung von Dateien in mehrere Streams.

In Windows 9x beispielsweise existiert lediglich ein Stream, der Programm-Code selbst. Windows NT/2000 ermöglicht es dagegen, eine Datei über mehrere Streams (über filename:streamname) anzusprechen. Zu diesen können unabhän-

gig ausführbare Programm-Module oder auch Service-Streams (Zugriffsrechte, Verschlüsselungsdaten, Verarbeitungszeit und so weiter) zählen. Dieses Merkmal macht das NTFS-Dateisystem sehr vielseitig verwendbar, da sich für spezifische Aufgabenstellungen jeweils angepasste Daten-Streams erzeugen lassen.




**So arbeitet W2K.Streams:** Der Virus ersetzt den Haupt-Stream der Datei durch seinen Code.

W2K.Stream ist der erste bekannte Virus, der dieses Feature nutzt, um über multiple Streams Dateien auf NTFS-File-Systemen zu infizieren. Dazu erzeugt der neue Virus einen Stream namens STR und kopiert den ursprünglichen Datei-Inhalt dorthin. Dann ersetzt er den Haupt-Stream durch den Virus-Code. Wird das so infizierte Programm später gestartet, übernimmt der Virus die Kontrolle und beginnt mit seiner Replikation in andere Daten-Streams. Anschließend übergibt er durch die Erzeugung eines neuen Prozesses für filename:STR die Kontrolle an den eigentlichen Programm-Code.

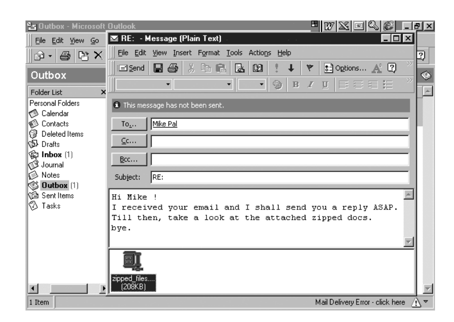
## 3.3.7 Würmer

Würmer infizieren keinen fremden Code, um sich fortzupflanzen. Vielmehr sind sie auf die selbstständige Verbreitung in Netzwerken ausgerichtet, wodurch sie sich von Viren und Trojanern unterscheiden.

Bekannte Vertreter dieser Spezies sind W32/Klez-H, W32/ExploreZip, W32/Ska (auch als Happy99 bekannt) oder W32/PrettyPark. Der Präfix W32 bedeutet, dass es sich um 32-Bit-Programme für Windows 9x und NT handelt.

Unter dem Namen ExploreZip beziehungsweise ZippedFiles verbreitete sich Anfang Juni 1999 ein solcher Wurm für Windows-9x-Systeme. Das Opfer bekommt eine englischsprachige E-Mail mit persönlicher Anrede, an die eine .exe-Datei mit dem Namen ZippedFiles angehängt ist. Das wirkt wie ein normales Zip-Archiv, das sich per Doppelklick öffnen lässt. Stattdessen aktiviert ein Doppelklick den Wurm. Der gibt eine Fehlermeldung aus, die ein korruptes Zip-Archiv bemängelt.

Im Hintergrund kopiert der Wurm eine Datei namens explore.exe in das System-Verzeichnis von Windows und verändert die Datei win.ini. Damit wird der Wurm bei jedem PC-Start aktiv.




**Tarnung ist alles:** Der Wurm ExploreZip verschickt sich selbst an die Personen im Outlook-Adressbuch.

Dann wartet er auf den Start von Outlook, durchsucht den Posteingang und schickt allen Absendern eine Antwort. Dabei benutzt er den Vornamen als Anrede und verspricht eine baldige Antwort auf die ursprüngliche E-Mail. In der Zwischenzeit soll der Empfänger einen Blick auf das angehängte Zip-Archiv werfen – schon ist ein neuer PC infiziert.

Der Schaden, den ExploreZip anrichten kann, ist enorm. Er durchsucht gezielt alle verfügbaren Laufwerke, auch im Netz, nach Quelldateien diverser Programmiersprachen sowie Word-, Excel- und PowerPoint-Dokumenten. Anschließend setzt es die Länge dieser Dateien auf Null. Das erschwert – im Gegensatz zum einfachen Löschen – das Wiederherstellen der Dateien erheblich.

## 3.3.8 Siegeszug der Internet-Würmer

Äußerst erfolgreich behaupten sich seit Code Red Würmer, die zu ihrer Verbreitung bekannte Windows-Sicherheitslücken nutzen. Und das, obwohl Microsoft für diese Schwachstellen bereits entsprechende Patches herausgebracht hat.

So ist am 18. September 2001 mit W32/Nimda ein äußerst aggressiver Wurm aufgetreten. Er nutzt zwei bekannte Sicherheitslücken im Internet Explorer und Internet Information Server, um sich über 32-Bit-Windows-Systeme fortzupflanzen. So sorgt etwa der manipulierte MIME-Header von HTML-Mails dafür, dass bereits bei der Vorschau einer Nachricht in Outlook (Express) das verseuchte Attachment readme.exe ausgeführt wird. Einmal aktiv, verschickt sich der Parasit über einen eigenen SMTP-Server an weitere Opfer. Deren E-Mail-Adressen extrahiert der Wurm aus HTML-Seiten oder über MAPI aus der Inbox des Mail-Client.

Nimda befällt ebenfalls den Microsoft Internet Information Server, indem er mit Hilfe von Portscans verwundbare Rechner im Internet aufspürt. In deren Webseiten baut der Schädling JavaScript-Code ein, der beim Besuch einer solchen Seite

die präparierte Datei readme.eml auf den lokalen Rechner lädt und sie ausführt. Gegen diese Gefahr hilft das Deaktivieren der JavaScript- und Download-Funktion im Browser.

Der Wurm kann sich auch über Windows-Freigaben ausbreiten, die er für jedes lokale Laufwerk versteckt anlegt. Findet Nimda im Netzwerk Shares mit Schreibzugriff, erzeugt er auf diesen Laufwerken Kopien von sich im NWS- oder EML-Format. Der dabei gewählte Dateiname wird zufällig generiert.




**Wie ein Lauffeuer:** Binnen 24 Stunden breitete sich W32/Nimda weltweit auf Zehntausenden von Rechnern aus.

Obwohl für die Schwachstellen, über die der Schädling eindringt, seit geraumer Zeit Patches verfügbar sind, hat sie offenbar kaum jemand eingesetzt. So konnte sich der Wurm rasant verbreiten und weltweit die Computernetze verstopfen.

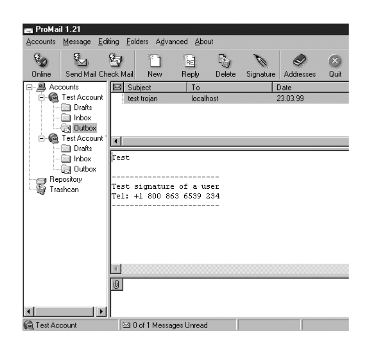
W32/Klez, der sich 2002 schnell verbreitete, nutzt die IFRAME-Sicherheitslücke des Internet Explorer aus, um sich beim Betrachten einer E-Mail per Outlook automatisch zu installieren. Als Erstes deaktiviert er Anti-Virus-Software mittels der Windows-API „TerminateProcess“, um sich dann über das Windows-Adressbuch und einen eigenen SMTP-Client weiter zu verbreiten. Zudem infiziert er lokale und über Windows-Freigaben erreichbare Dateien.

## 3.3.9 Trojaner

Während sich Viren und Würmer nach Möglichkeit verstecken, treten Trojanische Pferde offen auf. Sie geben sich als Bildschirmschoner, Passwortverwaltung oder ein anderes nützliches Tool aus. Diese Funktion erfüllen Trojaner gelegentlich sogar mehr oder weniger gut. Meistens geht es aber lediglich darum, den Empfänger dazu zu verlocken, die Malware zu starten, so dass der Schädling zuschlagen und dabei die Festplatte löschen sowie einen Bootvirus oder ein Remote-Administrationstool installieren kann.

Ein besonders krasses Beispiel: Anfang 1998 entschlüsselten zwei 16-jährige Kölner Realschüler, Aaron Spohr und Marcel Henning, die Verschlüsselung des T-Online-Passworts. Anschließend programmierten sie die T-Online Power Tools, ein Hilfsprogramm für den T-Online-Decoder, das rasch Verbreitung fand. Sobald jemand die Online-Registrierung benutzte, schickte der Trojaner über das Internet auch die Zugangsdaten zum jeweiligen T-Online-Anschluss mit. Die Verschlüsselung des Decoders war nur mangelhaft. So kamen in kurzer Zeit 600 Passwörter zusammen. Zum Glück für die Ausgespähten ging es den Schülern nur darum, die Machbarkeit nachzuweisen. Sie veröffentlichten ihre Erkenntnisse in der Presse.

Ähnlich arbeitet das Freeware-E-Mail-Programm ProMail 1.21. Erwartungsgemäß tippt der Anwender die Zugangsdaten für seinen Mail-Account ein. Diese Daten schickt das Programm im Hintergrund an eine E-Mail-Adresse. Damit kann der Urheber die elektronische Post seiner Opfer abrufen.




**Getarnt als Freeware:** Das E-Mail-Programm ProMail versendet „heimlich" Informationen zu den POP-Accounts an eine anonyme Adresse.

Der Trojaner Back Orifice nistet sich im Systemkern von Windows ein. Dann wartet das Programm, bis es ein Hacker über das Internet aktiviert. Dabei lässt es den ungebetenen Gast Dateien kopieren, sämtliche Tastatureingaben mitlesen, Programme starten und vieles mehr. Es ist zu erwarten, dass in Zukunft mehr solcher „Tools" in Umlauf gebracht werden. Auch vor solchen Programmen sollte Sie ein gutes Antiviren-Programm schützen.

### 3.3.10 Enten: Hoaxes

Im Bestiarium der Schadensprogramme, auch als Malware bezeichnet, gibt es noch eine weitere Variante: Hoaxes. Als deutsche Übersetzung trifft „Ente“ wohl den Kern der Sache. Ein Hoax ist eine gezielte Falschmeldung per E-Mail über einen Virus oder ein anderes Schadensprogramm. In der Regel wird der Empfänger aufgefordert, die E-Mail an alle Bekannten als Warnung weiterzuleiten. Und genau das ist die Schadenswirkung eines Hoax: Er kostet Arbeitszeit in Firmen und verbreitet sich rasend schnell.

Einer der ersten Hoaxes tauchte mit „GoodTimes“ Ende 1994 auf. Die Mail warnte vor einem Virus, der alleine durch Lesen einer E-Mail einen PC infizieren könne. Erkennbar sei die Nachricht durch die Worte „Good Times“ im Betreff. Der Virus würde dann den Festplatteninhalt löschen oder gar den Prozessor des Computers zerstören. Ins Deutsche übersetzt liest sich die englische Originalnachricht über Good Times so: FYI: Eine Datei mit dem Namen „Good Times“ wird von einigen Internet-Usern versendet, die bei Online-Services (CompuServe, Prodigy und AOL) angemeldet sind. Wenn Sie diese Datei empfangen sollten, NICHT downloaden! Sofort löschen. Ich weiß, dass in dieser Datei ein Virus enthalten ist, der, sofern auf Ihren PC geladen, alle Ihre Dateien ruiniert.

Als besonders hartnäckig erweist sich das Gerücht über einen Virus, der durch das Vorhandensein der Datei jdbgmgr.exe erkannt werden könne. In der Mail wird dazu aufgefordert, diese Datei sofort zu löschen. Tatsächlich ist diese Datei wichtiger Bestandteil der Java-VM von Windows.

Nach diesem Muster funktionieren alle gängigen Falschmeldungen über vermeintliche Viren. Oft findet sich im Text der entsprechenden Mail noch der Hinweis, dass namhafte Computerfirmen die Warnung vor dem neuen Virus ausgegeben hätten. Eine ständig aktualisierte Übersicht von Hoaxes findet sich beispielsweise auf den Internet-Seiten der TU Berlin (www.tu-berlin.de/www/software/hoax.shtml). Daneben wird man ebenfalls bei den großen Antivirenherstellern fündig, wie etwa bei Network Associates (www.nai.com) oder Symantec (www.symantec.com).

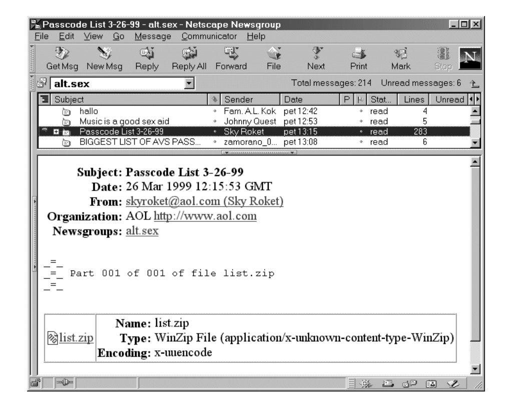
### 3.3.11 Makroviren

In den letzten Jahren sind Makroviren zur größten Gefahr geworden. Denn das Office-Paket von Microsoft verfügt über eine ausgefeilte Makrosprache mit mächtigen Befehlen: VBA, Visual Basic für Applikationen. Mit diesen Befehlen kann ein Makro zum Beispiel Dateien und andere Office-Dokumente manipulieren oder Windows-Programme fernsteuern.

Der Knackpunkt bei MS-Office: Die Makros sind direkt im Dokument gespeichert. Wenn Sie ein WinWord-, Excel- oder PowerPoint-Dokument weitergeben, sind eventuell Makros mit dabei. Und es gibt eine Autostart-Funktion. Sobald Sie ein Dokument mit einem entsprechend deklarierten Makro öffnen, wird das Ma-

kro aktiv. Dann verändern die meisten Makroviren die Standard-Dokumentvorlage normal.dot so, dass der Virus bei jedem Start von Word aktiv wird. Die Vorgehensweise bei den anderen Office-Applikationen basiert auf demselben Prinzip.

Besondere Brisanz haben Makroviren, die sich selbstständig über E-Mail weiter verbreiten. Das bekannteste Beispiel dafür ist Melissa: Der Virus sucht sich aus der Outlook-Datenbank 50 Empfänger aus und schickt ihnen eine E-Mail mit dem Virus als Anhang. Wenn die Empfänger den Anhang per Doppelklick aktivieren, nistet sich Melissa im System ein. Dass die E-Mail von einem bekannten Absender stammt, vergrößert die Chance auf einen unbedachten Doppelklick. Mittlerweile gibt es etliche Nachahmer, auch für Excel.




**Infektionsquelle Newsgroup:** Ungeschützter Verkehr ist auch im Cyberspace riskant.

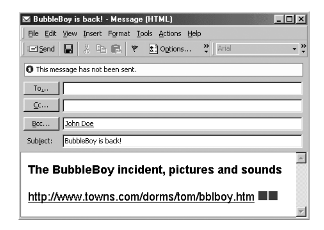
Der Schaden, den Makroviren anrichten können, ist beträchtlich. Denken Sie beispielsweise an eine große Excel-Tabelle mit einer statistischen Auswertung. Ein Virus könnte hier zufällig einige Werte ändern, in einen WinWord-Text Tippfehler einbauen oder einzelne Wörter ersetzen. Der Aufwand, die Originaldaten wieder herzustellen, kann enorm sein.

## 3.3.12 Sicherheitsrisiko VBScript

Eine der brennendsten Fragen zu Viren und Internet: Kann ich mir einen Virus einfangen, indem ich einfach nur eine Webseite aufrufe oder eine E-Mail empfange? Generell gesagt: nein. Die beiden Programmiersprachen des WWW, Java und JavaScript taugen nicht zur Verbreitung von Viren. Abgesehen von Sicherheitslücken, die in der Regel rasch durch Updates geschlossen werden, lassen sie keinen Zugriff außerhalb des Browsers auf das System zu.

Ganz anders sieht das mit VBScript aus. Diese Untermenge von Visual Basic hat Microsoft in seinen Internet Explorer eingebaut – andere Browser unterstützen es nicht. VBScript lässt weit reichende Zugriffe auf das System zu, etwa die Manipu-

lation von Dateien oder der Registry. Auch hier können zusätzliche Schwachstellen in Form von Sicherheitslücken auftreten, die beispielsweise VBS/BubbleBoy zum Zugriff auf die Festplatte nutzt.




**Sonderfall BubbleBoy:** Dieser VBScript-Virus wird durch eine Sicherheitslücke von Outlook schon beim Lesen der E-Mail aktiv.

Allerdings hängen diese Fähigkeiten von vielen Randbedingungen ab. Laden Sie eine Webseite aus dem Internet, erlaubt der Internet Explorer einem VBScript keine Eingriffe ins System. Anders sieht die Sache aus, wenn Sie eine HTML-Datei von der lokalen Festplatte öffnen. Wenn die Sicherheitseinstellungen des Internet Explorer auf „Sehr niedrig" eingestellt sind, kann ein VBScript-Virus Dateien auf der Festplatte ändern. Weil immer mehr Programme ihre Online-Hilfe im HTML-Format mitliefern und auch die Windows-Hilfe selbst in HTML programmiert ist, handelt es sich dabei um eine reale Gefahr. Unser Testvirus HTML.Reality infiziert zum Beispiel sämtliche HTML-Dateien in bestimmten Systemlaufwerken, setzt die Sicherheitseinstellungen des Internet Explorer zurück und schreibt dann einen klassischen Virus ins System. Zu allem Überfluss hat der Internet Explorer keine getrennten Einstellungen für JavaScript und VBScript. Unter der Option „Scripting" können Sie nur alle Scripts deaktivieren oder erlauben.

## 3.3.13 Vorbeugen gegen Viren

Absolut sicher sind Sie vor Viren nur, wenn Sie keine fremden CDs und Disketten in Ihren PC stecken und auch keine Dateien aus dem Internet laden – aber wer will das schon? Selbst originalverpackte Programme direkt vom Hersteller sind gelegentlich infiziert. 1998 hat Corel mit der Mac-Version von Corel Draw 8.0 unwissentlich einen Virus ausgeliefert; Microsoft verteilte 1995 unabsichtlich einen der ersten WinWord-Makroviren WM/Concept mit einem Dokument auf einer Probe-CD.

Mit einem gewissen Maß an Vorbereitungen ist man Viren trotzdem nicht hilflos ausgeliefert. Die folgenden Regeln stellen zwar keine Garantie dar, schränken Infektionswege aber drastisch ein und begrenzen den Schaden im Ernstfall.

- Legen Sie mit der entsprechenden Funktion Ihres Antiviren-Programms eine bootfähige Notfalldiskette an. Verlassen Sie sich nicht auf die fertig mitgelieferte Diskette. Diese ist häufig nicht bootfähig. Stellen Sie sicher, dass Sie Installationsdisketten oder -CDs von Windows und den wichtigen Program-

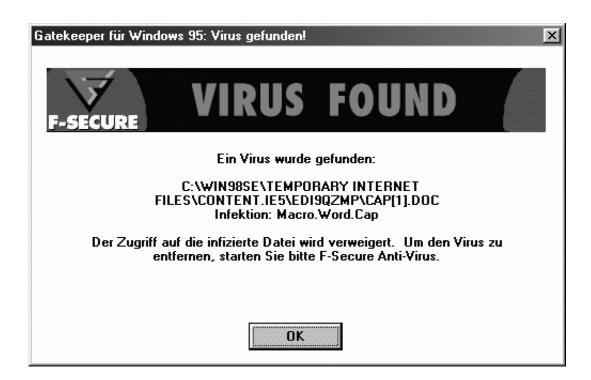
men griffbereit haben. Außerdem brauchen Sie zur Sicherheit eine DOS- oder Windows-Startdiskette mit CD-ROM-Treibern.

- Machen Sie regelmäßig Backups wichtiger Daten und Dokumente – ihre Wiederherstellung kostet viel Zeit und Mühe. Windows und Programme lassen sich relativ leicht wieder installieren. Noch besser: Bewahren Sie mehrere Backup-Versionen auf.
- Schalten Sie im BIOS das Booten von Diskette aus. Damit ist das Risiko, sich einen Bootvirus von einer Diskette einzufangen, praktisch auf Null reduziert. Im Bedarfsfall lässt sich die Boot-Reihenfolge leicht wieder umstellen.
- Lassen Sie im Hintergrund immer einen Virenwächter mitlaufen.
- Durchsuchen Sie die ganze Festplatte regelmäßig, mindestens einmal die Woche, mit dem Virenscanner. Nutzen Sie dazu den Terminplaner des Scanners.
- Besorgen Sie sich regelmäßig Updates für Ihren Virenscanner. Nur so findet er auch neue Viren.
- Achten Sie auf ungewöhnliche Reaktionen Ihres PCs, sie könnten ein Anzeichen für eine Infektion sein.

## 3.3.14 Virenscanner

Moderne Antivirenprogramme bestehen aus On-Demand-Scanner und On-Access-Scanner, auch Virenwächter genannt. Der On-Demand-Scanner untersucht nach dem Start die virusgefährdeten Dateien auf Datenträgern. Da ein Virenscanner nur Sinn macht, wenn man ihn regelmäßig benutzt, ist ein Zeitplaner Standard. Er gibt vor, an welchen Tagen und zu welcher Uhrzeit der Scanner aktiv wird.

Der On-Access-Scanner läuft als Betriebssystemtreiber im Hintergrund und untersucht bei jedem Zugriff auf eine Datei, ob ein Virus enthalten ist. Zudem sind einzelne Wächterprogramme in der Lage, auch Online-Verbindungen und den E-Mail-Datenverkehr zu prüfen.




**Aufmerksamer Wächter:** Der Virenwächter von F-Secure Antivirus hat entdeckt, dass der Internet Explorer eine virenverseuchte Datei im temporären Verzeichnis angelegt hat.

Virenscanner erkennen nur die Schädlinge sicher, die bereits bekannt sind. Deshalb ist es entscheidend, dass Sie sich regelmäßig Updates der Virensignaturen besorgen. Die Signatur ist das typische Merkmal eines Virus, anhand dessen der Virenscanner eine befallene Datei erkennt. Mindestens einmal pro Woche ist ein Update fällig. Am praktischsten sind Virenscanner, die sich die Aktualisierungen selbst über das Internet besorgen.

Noch weiter geht die heuristische Suche, die Programme auf virentypische Befehlssequenzen prüft. Das ist besonders für polymorphe Viren wichtig, und auch für Makroviren sollte so eine Heuristik vorhanden sein. Mit dieser Technik kann der Scanner auch neue Viren als verdächtig deklarieren. Derartige Dateien schicken Sie am besten per Internet an den Hersteller, der dann innerhalb kurzer Zeit ein Update verfügbar macht.

## 3.3.15 Was tun bei Virenbefall?

Bei einem Virenvorfall gilt es, zwei Zustände zu unterscheiden: Entweder der Virenscanner hat eine Datei oder Diskette mit einem Virus entdeckt, dieser ist jedoch noch nicht aktiv. Oder aber der Scanner entdeckt einen Virus, der bereits im System aktiv ist.

Im ersten Fall ist der Virenscanner meistens in der Lage, den Virus zu entfernen, bevor er Schaden anrichtet. In manchen Fällen geht dabei aber die befallene Datei verloren, weil der Virus Teile davon unwiederbringlich überschrieben hat. Ist der Virus bereits aktiv, sollten Sie vorsichtig vorgehen und die nachfolgende To-do-Liste berücksichtigen:

- Bei einem Virenbefall gilt vor allem eins: Keine Panik, die erforderlichen Maßnahmen in Ruhe ergreifen. Das Formatieren der Festplatte ist die allerletzte Aktion – und bestimmte Viren überstehen sogar das.
- Wie alt ist das letzte Backup? Im Zweifelsfall legen Sie sofort eine aktuelle Datensicherung an – ohne die letzte zu überschreiben! Denn eine virenverseuchte Sicherung ist besser als gar keine. Wenn etwas schief geht, kann ein Profi vielleicht die Daten retten. Ein Disk Imager wie beispielsweise Drive Image (www.powerquest.com) oder Ghost (www.symantec.de) sichert den gesamten Festplatteninhalt.
- Nehmen Sie das Handbuch Ihres Antiviren-Programms zur Hand und lesen Sie genau durch, was dort für den Ernstfall empfohlen wird. Bisweilen kommt es nämlich darauf an, mit welchem Betriebs- und Dateisystem (Windows NT mit NTFS, Windows 95B mit FAT32X et cetera) Sie arbeiten.
- Bei Bootviren gilt: Erst jetzt sollten Sie daran gehen, den PC mit der Notfalldiskette Ihres Antiviren-Programms beziehungsweise der DOS- oder Windows-Startdiskette zu booten. Nur so ist gewährleistet, dass kein Virus aktiv ist. Achten Sie aber darauf, dass der Schreibschutz-Schieber der Diskette aktiviert ist.

## 3.3.16 Nicht vergessen: Nachsorge

- Um zu verhindern, dass der Virus in einer versteckten Datei überlebt und später erneut wichtige Dateien infiziert, sollten Sie alle Laufwerke einer genauen Prüfung mit dem Virenscanner unterziehen.
- Versuchen Sie auch festzustellen, woher der Virus kam: via E-Mail, per Dokument auf Diskette oder über Downloads aus dem Internet. Benachrichtigen Sie den Absender oder Anbieter mit möglichst genauen Angaben.
- Stellen Sie den Zeitplaner Ihres Virenscanners so ein, dass er täglich einen kompletten Scan aller Laufwerke durchführt. Damit verhindern Sie die Neuinfektion aus einem bisher nicht entdeckten „Rückzugsgebiet" des Virus.
- Bei Makroviren sollten Sie sich über den Virus und seine Schadensfunktion in der Virendatenbank Ihres Scanners oder auf der Webseite des Herstellers informieren. Denn es kann sein, dass der Virus den Inhalt von Dokumenten manipuliert hat. Es besteht die Gefahr, dass Sie mit den veränderten Daten weiterarbeiten.

## 3.3.17 Fazit

Die Bedrohung durch Viren, Würmer und Trojaner dürfte weiterzunehmen. Selbst Laien können heutzutage Sabotage-Programme mit Hilfe von Construction-Kits erstellen: Über ein komfortables Frontend lassen sich Schädlinge nach dem Baukastenprinzip zusammenklicken. Auf diese Weise generierte Malware ist oft erstaunlich effektiv. Als E-Mail-Anhang verbreiten sich die digitalen Parasiten in Windeseile über das Internet. Eine eindeutig gewählte Betreffzeile – etwa „Sex Pics for free" – sorgt dafür, dass möglichst viele Empfänger alle Vorsicht fahren lassen und das verseuchte Attachment starten. Ein sicherer Schutz vor Viren bedarf einer gewissen Selbstdisziplin. Virenscanner müssen up to date gehalten werden, auf manch komfortables Software-Feature sollte man besser verzichten und nicht alles, was klickbar ist, sollte auch geöffnet werden. Doch wer sich an ein paar Grundregeln hält, ist auch künftig vor Virenangriffen weit gehend sicher.

Wolfgang Nefzger, Thomas Rieske, Mike Hartmann

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Virentrends: Die Entwicklung der digitalen Plagegeister | a86 | – |
| Virenscanner im Test | a214 | – |
| Report: Viren unter Linux | a681 | – |
| ILOVEYOU: Hilfe und Hintergründe | a393 | – |
| Windows 2000 Bugreport | a317 | – |
| Aktuelle IE-Sicherheitslücken | a185 | – |

## 3.4 Sicher im Web unterwegs

Ausgespähte Passwörter, virenbehaftete Mailanhänge oder untergeschobene 0190-Dialer: Die bunte Internet-Welt birgt viele Gefahren, insbesondere wenn der Rechner in einem LAN hängt und damit gleichzeitig die gesamte Netzwerk-Infrastruktur der Firma gefährdet. Einige grundlegende Vorsichtsmaßnahmen bei den Nutzern helfen, das Risiko zu minimieren.

Das Internet ist keine Einbahnstraße. Jeder ans weltweite Datennetz angeschlossene Rechner wird Teil dieses Netzes, und sei es nur temporär. Während dieser Zeit stehen seine Ressourcen prinzipiell allen anderen Usern zur Verfügung – er wird damit angreifbar.

Schwachstellen gibt es auf einem typischen Windows-System genügend: Das Gespann aus Internet Explorer und Outlook ist mit seiner umfangreichen Unterstützung von Script-Sprachen sowie bedenklichen Default-Einstellungen ein beliebtes Einfallstor von Malware. Genauso wie der Windows Script Host, der standardmäßig ohne Rückfrage VBS- und JavaScript-Dateien ausführt. Wir zeigen Ihnen, wie sich diese neuralgischen Punkte entschärfen lassen. Ein Virenscanner gehört zwar zur Grundausstattung eines Rechners, ein Allheilmittel ist er aber nicht. Er wirkt nur gegen bekannte Viren, Würmer und Trojaner. Ein regelmäßiges Update der Signaturdateien ist also Pflicht.

Überdies richten alle technischen Sicherheitsmaßnahmen gegen leichtsinniges Verhalten der Anwender wenig aus. Dass man Passwörter nicht auf einen Zettel schreibt und unter die Tastatur klebt, scheint sich zwar langsam herumzusprechen; weniger jedoch, dass auch deren Wahl wohl überlegt sein will: Der Name der Ehefrau oder Freundin jedenfalls eignet sich denkbar schlecht. Dabei gibt es eine einfache Methode, wie man sich Passwörter so aussucht, dass diese nicht so leicht zu knacken sind.

Ohne eine Anfälligkeit der User für Social Engineering wären auch 0190-Dialer kaum derart erfolgreich. Die Anbieter versuchen fast immer mit derselben Masche, den Surfern die teuren Wählprogramme unterzuschieben: Ein Link verspricht kostenlosen Zugang zu viel nackter Haut. Eine gesunde Portion Misstrauen und ein paar technische Vorkehrungen verhindern, dass die Telefonrechnung in astronomische Höhen steigt.

Mag ein leichtsinniges Verhalten eines Privat-Users nur seinen eigenen PC gefährden, so kann eine Unachtsamkeit bei Rechnern im LAN schon zu einer mittleren Katastrophe für eine Firma führen, wenn ein Virus plötzlich das gesamte Netz verseucht oder ein Trojaner fleißig Unternehmensdaten ins Internet schickt. Natürlich kann man jetzt ganz einfach jedem Angestellten den Internet-Zugriff komplett sperren, aber das ist angesichts der Recherchemöglichkeiten und dem damit verbundenen Weiterbildungseffekt sicherlich nicht allzu produktiv.

Die andere Option ist ein Proxy-Server mit Virenscanner im LAN, über den alle Zugriffe abgewickelt werden. Dennoch bleibt ein Restrisiko durch unbekannte Sicherheitslücken und neue Viren. Deshalb hilft hier nur eine gründliche Einweisung der Benutzer, Hinweise auf Gefahrenpotenziale und allgemeine Verhaltensrichtlinien für den Umgang mit dem Internet.

## 3.4.1 Browsen – aber sicher

Aktuelle Browser sind wahre Alleskönner, mit denen sich nicht nur HTML-Seiten betrachten lassen. Sie interpretieren auch aktive Inhalte wie Java, JavaScript, ActiveX oder Visual Basic Script (VBS).

Zwar sind Sicherheitsmechanismen vorgesehen, die verhindern sollen, dass Unberechtigte Dateien auf dem PC des Anwenders verändern, löschen oder auslesen. Doch immer wieder tauchen in den Implementationen der Browser-Hersteller neue Sicherheitslücken auf. Durch die enge Verzahnung mit Mail- und News-Client wie beim Internet Explorer machen sich die Schwachstellen gleich auch bei diesen Komponenten bemerkbar.

Daher sollte man sehr zeitnah die Patches oder Updates aufspielen, die den entdeckten Bug beseitigen. Es empfiehlt sich also, regelmäßig auf den entsprechenden Webseiten der Hersteller nachzuschauen. Microsoft etwa informiert über Sicherheitsprobleme auf der Technet-Seite (www.microsoft.com/technet/), auf der man auch die Security Bulletins abonnieren kann.




**Ernst zu nehmende Warnungen:** Patches, die der Hersteller anbietet, sollte man auch installieren.

Die Redmonder wollen allerdings detaillierte Hinweise über Sicherheitslücken erst veröffentlichen, nachdem ein Patch bereits mindestens 30 Tage erhältlich ist. Um trotzdem frühzeitig Gefahren abschätzen zu können, lohnt sich somit auf jeden Fall ein Abonnement der Bugtraq-Mailingliste (www.ntbugtraq.com).

## 3.4.2 Das Zonenmodell des Internet Explorer

Selbst ohne akute Sicherheitslöcher sorgen aktive Inhalte für genügend Gefahrenpotenzial. Daher benutzt der Internet Explorer seit Version 4 ein Sicherheitsmodell, um Websites in unterschiedlich vertrauenswürdige Zonen einzuteilen. Der Benutzer ordnet Websites einer der vier Zonen „Lokales Intranet", „Internet", „Vertrauenswürdige Sites" oder „Eingeschränkte Sites" zu, für die jeweils andere Sicherheitsvorgaben gelten. Die Herkunft der riskanten ActiveX-Controls bewertet der Internet Explorer anhand von digitalen Zertifikaten.

Dem lokalen Intranet ordnet der Internet Explorer Sites zu, die er ohne Proxy-Server oder über einen UNC-Netzwerkpfad ansprechen kann. Diese Zone ist in erster Linie für Firmen interessant, die im LAN Webserver einsetzen und über einen Proxy mit dem Internet verbunden sind.

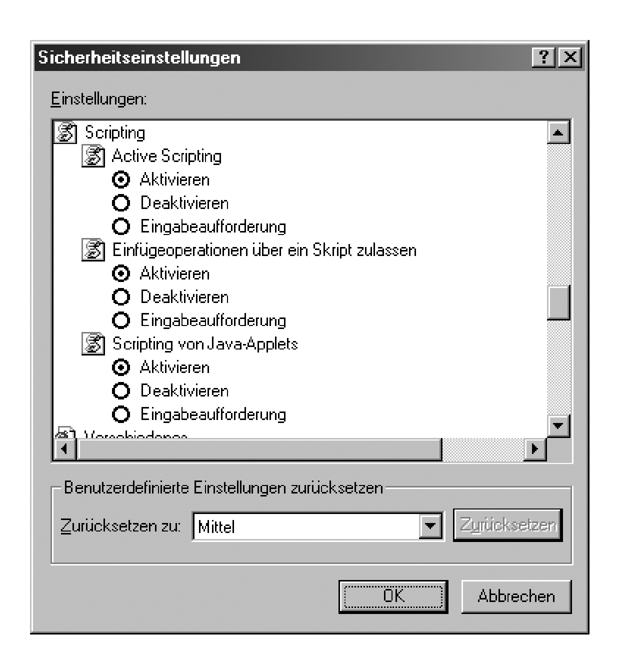



**Höchste Sicherheitsstufe:** Die Zone „Eingeschränkte Sites" des Internet Explorer muss der Anwender selbst mit Einträgen füllen.

Die beiden Listen für vertrauenswürdige und eingeschränkte Sites sind standardmäßig leer: Die Einträge muss der Anwender selbst vornehmen. Unter der Zone „Internet“ fasst der Browser alle übrigen Sites zusammen. Über die Registerkarte „Sicherheit“ der Internet-Optionen lässt sich für jede Zone detailliert festlegen, wie der Internet Explorer mit potenziell schädlichen Inhalten umgehen soll. Die Einstellungen sind Microsoft-typisch verschachtelt aufgebaut und erlauben nicht unbedingt Feineinstellungen. So hat Microsoft unter „Active Scripting“ JavaScript und VBS zusammengewürfelt. Wer nur eine der Script-Sprachen abschalten will, hat dazu keine Möglichkeit.

### 3.4.3 IE-Zonenmodell: Vorgaben

Microsoft hat die Sicherheitsoptionen zu Standardvorgaben von „sehr niedrig“ bis „hoch“ zusammengefasst und als Vorgabe jeder Internet-Zone eines dieser Settings zugewiesen. Die vertrauenswürdigen Sites behandelt der Internet Explorer (IE) mit „sehr niedrigen“, die lokale Intranet-Zone mit „niedrigen“, die Sites der Internet-Zone mit „mittleren“ und die eingeschränkten Sites mit „hohen“ Sicherheitseinstellungen.



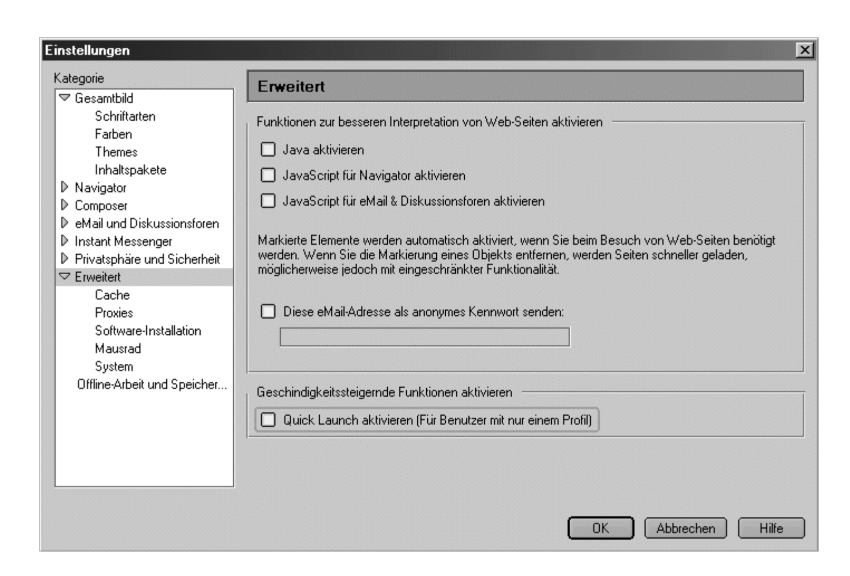

**Schwache Vorgabe:** Den Sites in der Internet-Zone gestattet der Internet Explorer das Ausführen von Scripts.

In der wohl wichtigsten Zone „Internet" lässt der Browser damit Java, JavaScript, VBS und ActiveX-Controls zu – eine sehr fahrlässige Vorgabe. Stattdessen empfiehlt es sich, die Sicherheit in der Standardzone auf „hoch" zu setzen. Bei IE-Versionen vor 6.0 sollten Sie außerdem unter „ActiveX-Steuerelemente und Plugins" sämtliche Schalter deaktivieren.

Für einige Webangebote muss der Surfer die rigiden Vorgaben außer Kraft setzen – etwa weil die Online-Bank JavaScript voraussetzt. Zu diesem Zweck kann der Anwender die betreffenden Server in die Zone der vertrauenswürdigen Sites eintragen. Allerdings empfiehlt es sich, hier wirklich nur die Webangebote bestens bekannter Betreiber einzutragen.

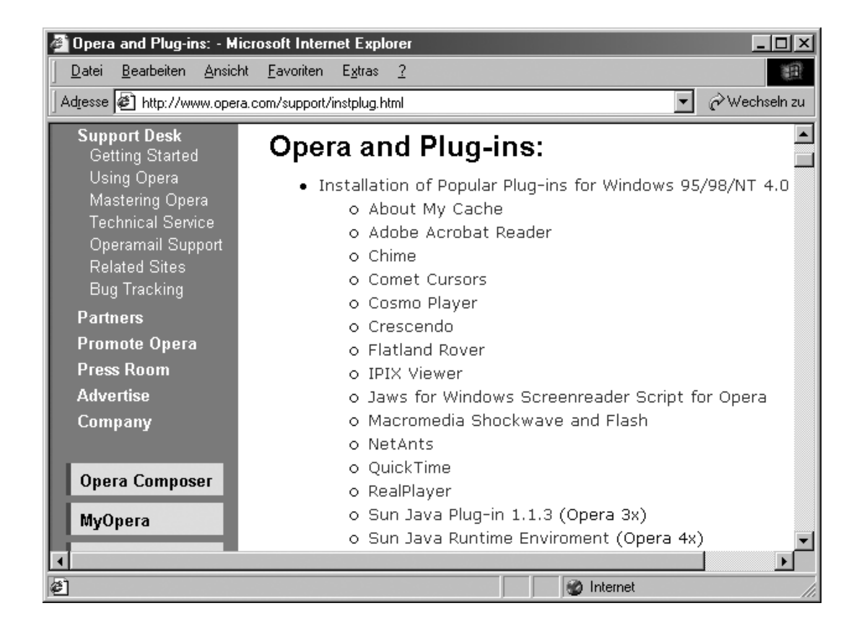
## 3.4.4 Alternativen: Netscape und Opera

Wer statt auf den Internet Explorer auf Mozilla (www.mozilla.org) und Opera (www.opera.com) setzt, hat ein paar Sorgen weniger. Denn die beiden Konkurrenten unterstützen weder ActiveX noch VBS – ein klarer Vorteil in punkto Sicherheit. Ein Zonenmodell, wie vom Internet Explorer bekannt, verwenden Netscape und Opera nicht. Somit lassen sich Java und JavaScript immer nur generell abschalten und bei Bedarf wieder aktivieren.




**Entweder – oder:** Netscape kennt kein Zonenmodell, über das sich Websites verschiedenen Bereichen zuordnen lassen. Die Einstellungen gelten nur global.

Der Netscape Communicator 4.78 hatte Java noch fest integriert, seit den 6.x-Versionen unterstützen diese und andere Erweiterungen lediglich als Plug-ins – ebenso Opera. Diese Zusätze sollte man sich generell von den jeweiligen Herstellerservern herunterladen, was das Risiko, sich Malware einzufangen, minimiert.




**Reiche Auswahl:** Opera bietet eine breite Palette von Plug-ins für den Browser.

Bei Opera hat der Surfer unter „Datei/Einstellungen" Zugriff auf sämtliche sicherheitsrelevanten Optionen – auch wenn sich diese wie die Checkboxen „Scriptsprachen benutzen" und „Java einschalten" nicht unter dem Punkt Sicherheit finden, sondern unter Plug-ins.

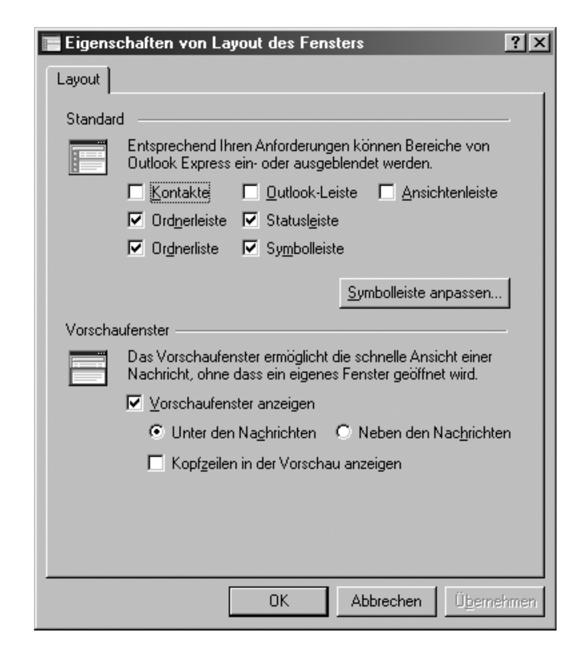
In Netscapes Sicherheitsbereich gelangt man, indem man die erweiterten Einstellungen aufruft. Hier lassen sich Java sowie JavaScript ein- und ausschalten, Letzteres getrennt für den Navigator sowie den Mail- und News-Client.

## 3.4.5 Outlook (Express)

Outlook und Outlook Express haben bei der Verbreitung von Viren und Würmern bislang stets eine tragende Rolle gespielt. Das liegt zum einen an der weiten Verbreitung dieser Programme: Viele Nutzer bedeutet viele potenzielle Opfer. Zum anderen sind der Internet Explorer und Outlook eng verknüpft: Microsofts Mail-Client greift zur Darstellung von Nachrichteninhalten auf die Rendering-Fähig-

keiten des Browsers zurück. Alles, was dieser interpretieren kann, wird bereits im Vorschaufenster ausgeführt. Das sind neben Grafiken aktive Inhalte wie ActiveX-Controls oder Visual-Basic-Scripts.

Um dem vorzubeugen, bietet Outlook unter „Extras/Optionen/Sicherheit" einige Einstellmöglichkeiten. Dazu gehört die Sicherheitszone, die der Mail-Client vom Internet Explorer übernehmen soll. Diese steht standardmäßig auf „eingeschränkte Sites". Wer sich nicht darauf verlassen mag, deaktiviert die automatische Vorschau unter „Ansicht/Layout" – was jedoch nur bei Outlook Express funktioniert. Outlook bietet diese Möglichkeit nicht.




**Outlook Express im Vorteil:** Beim kleinen Bruder von Outlook lässt sich das Vorschaufenster ausblenden.

Aus den oben genannten Gründen reagieren viele Menschen empfindlich auf Nachrichten im HTML-Format. Leider verwendet Outlook dieses Format standardmäßig, wenn Sie E-Mails schreiben oder in Newsgroups posten. Diese unsinnige Vorgabe sollten Sie daher unter den Senden-Optionen auf „Nur Text" umstellen.

Immerhin warnen beide Outlook-Varianten vor dem Öffnen ausführbarer Attachments. Weniger durchdacht ist hingegen die Möglichkeit, das „Speichern oder Öffnen von Anlagen, die möglicherweise einen Virus enthalten könnten" zu verhindern. Denn hiermit sperren Sie alle Attachments. Eine Ausnahmeliste wäre an dieser Stelle sinnvoller, so dass etwa reine Textdateien passieren dürften.

### 3.4.6 Starke und schwache Passwörter

Die Kombination aus User-ID und Passwort dient dazu, auf die unterschiedlichsten Ressourcen zuzugreifen, sei es der Fileserver im Unternehmen oder das Postfach eines Freemail-Anbieters. Eine gültige User-ID herauszufinden, ist recht einfach: Einige IDs, etwa „Administrator“, werden vom System vorgegeben. Bei anderen ist zumindest das Grundschema, etwa „vorname.nachname@firma.com“, bekannt. Das zugehörige Passwort zu knacken, ist für geübte Hacker ein Kinderspiel – wenn die Anwender es ihnen zu leicht machen.

Bei der Wahl eines Code-Worts sollte man immer daran denken, dass Angreifer mit minimalem Aufwand ein maximales Ergebnis erreichen wollen. Sie versuchen daher, so genannte schwache Passwörter aufzuspüren. Dazu zählen solche mit weniger als acht Zeichen, da sie zu anfällig für Brute-Force-Angriffe sind. Unsicher sind außerdem:

- Personen, Daten und Fakten aus dem Umfeld des Users, etwa der Name von Frau, Kind, Haustier, Lieblingsfilm, das Geburtsdatum oder Autokennzeichen
- lexikalisierte Begriffe, die ein lohnendes Ziel von Wörterbuchattacken sind
- nahe liegende Buchstaben-/Zahlenkombinationen (qwertz, abc123, q1w2e3r4)

Als Gegenstrategie auf zufällig generierte Passwörter wie f7{r&q_0 auszuweichen, dürfte allerdings eher kontraproduktiv sein. Denn diese vermeintlich sichere Verknüpfung aus Buchstaben, Zahlen und Sonderzeichen kann sich kaum jemand merken, schon gar nicht über längere Zeit. Als Konsequenz notieren sich die User das Passwort auf einem Zettel, den sie zweckmäßigerweise unter die Tastatur kleben oder idiotensicher an den Bildschirm.

Als besser zu handhaben erweist sich die Taktik, die Anfangsbuchstaben aller Wörter eines Ihnen bekannten Satzes zu wählen. So wird etwa aus dem Kinderreim „Punkt, Punkt, Komma, Strich – fertig ist das Mondgesicht“ das Passwort ppksfidm. Zusätzlich kann man noch die Groß- und Kleinschreibung sowie Satzzeichen berücksichtigen: P,P,K,S-fidM dürfte wirklich nicht einfach zu erraten sein.

### 3.4.7 Risiko Windows Script Host

Als Nachfolger für die aus DOS-Zeiten bekannten Batch-Dateien präsentierte Microsoft mit dem Windows Script Host (WSH) ein flexibleres Modell. Dieser Host interpretiert von Haus aus Visual Basic Script (VBS) und JavaScript (JS), lässt sich aber auch um weitere Module für Sprachen wie Perl oder Python erweitern.

WSH-Scripts bieten vielfältige Möglichkeiten, das System samt Applikationen fernzusteuern und dem Anwender lästige Routineaufgaben abzunehmen. Ein Zugriff auf die Registry lässt sich ebenso realisieren wie auf das gesamte Windows-Dateisystem. Kein Wunder, dass auch Programmierer von Malware den Script Host für ihre Zwecke nutzen. Ohne ihn hätten sich VBS-Würmer wie ILOVEYOU oder Anna Kournikova wohl kaum derart stark verbreitet.

Der WSH gehörte zwar bereits zum Lieferumfang von Windows 98 und 98SE, wurde aber nicht automatisch eingerichtet. Das hat sich mit der Millennium Edition (Me) geändert: Seitdem dient der Script Host als Default-Applikation für Dateien, die auf .js und .vbs enden.

Der in Windows XP enthaltene WSH 5.6, den es auch zum Download unter der Adresse http://msdn.microsoft.com/downloads/ für ältere Betriebssystemversionen gibt, versucht immerhin, den Gefahren mit Hilfe von Signaturen vorzubeugen: Sie sollen für die Integrität und Authentizität von Scripts bürgen.

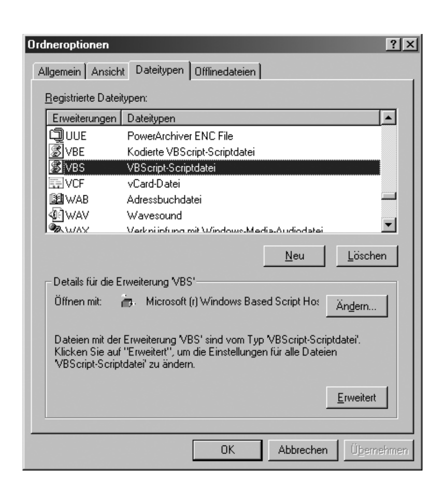
Beim Ausführen eines Scripts prüft der Script Host, ob es dafür eine Signatur gibt. Abhängig von der aktiven Sicherheitsstufe („Kein Schutz“, „Bei fehlender oder falscher Signatur warnen“ oder „Nur Skripte mit einwandfreier Signatur ausführen“) wird der Anwender gewarnt. Da derzeit aber erst wenige Scripts signiert sind, lautet die Default-Einstellung „Kein Schutz“.

### 3.4.8 Windows Script Host loswerden

Wer den Windows Script Host (WSH) nicht zwingend benötigt, sollte ihn am besten gleich deinstallieren. Problemlos gelingt das jedoch nur unter Windows 98: Über „Systemsteuerung/Software“ lässt sich die Komponente entfernen.

Ab Windows 98 SE hilft nur ein rigoroses Vorgehen, indem man die ausführbaren Dateien löscht oder zumindest umbenennt. Sie befinden sich im System32-Ordner des Betriebssystems: wscript.exe ist die GUI-Variante des Script Host, cscript.exe die Kommandozeilenversion.

Möchten Sie den WSH grundsätzlich behalten, aber verhindern, dass er Scripts direkt ausführt, können Sie die relevanten Dateitypen .vbs und .js an einen Editor wie Notepad binden. So lässt sich der Inhalt vorab auf Schadfunktionen kontrollieren.




**Verbindung lösen:** Statt mit dem Windows Script Host sollten die Script-Dateien zunächst mit einem Editor verknüpft werden.

Die neue Zuordnung nehmen Sie über den Windows-Explorer oder das Icon Arbeitsplatz im Menü „Ansicht/Ordneroptionen“ vor. Die Registerkarte „Dateitypen“ zeigt die aktuell gültigen Zuordnungen. Wählen Sie die Einträge „JScript-Scriptdatei“ respektive „VBScript-Scriptdatei“ und klicken auf „Bearbeiten“. In dem erscheinenden neuen Fenster wählen Sie den Eintrag „Öffnen“ und dann „Bearbeiten“. Hier lässt sich der Pfad zur gewünschten Applikation eintragen. Für Notepads ist das „C:\Windows\Notepad.exe“ beziehungsweise „C:\Winnt\Notepad.exe“. Wiederholen Sie diesen Vorgang für die kodierten Varianten der Script-Dateien (Datei-Namenserweiterungen .jse und .vbe).

### 3.4.9 0190-Dialer

Unternehmen, die ihre Dienste über 0190-Nummern bereitstellen, geraten stärker in Kritik. Schwarze Schafe schmuggeln auf den Rechner des Surfers Programme, die eine teure 0190-Verbindung aufbauen. Der dazu neu angelegte DFÜ-Eintrag drängt sich als Standard vor die ursprüngliche Provider-Verbindung oder trennt eine bestehende Verbindung. Mittlerweile hat sich auch die Politik des Problems angenommen. So forderte Verbraucherschutzministerin Künast, dass die horrenden Gebühren nur noch abgerechnet werden dürften, wenn der Kunde keinen Widerspruch einlegt. In der Tat können die Beträge extrem hoch ausfallen:

**Tarife der Deutschen Telekom**

| Rufnummer | Tarif | Preis (Euro / Min.) | Preis (Euro / Anwahl) | Davon für Anbieter (Euro / Min.) | Davon für Anbieter (Euro / Anwahl) |
|---|---|---|---|---|---|
| 0190-6x | T1 | 0,41 | – | 0,15 | – |
| 0190-5x | T2 | 0,62 | – | 0,34 | – |
| 0190-7x | T3 | 1,24 | – | 0,90 | – |
| 0190-8x | T4 | 1,86 | – | 1,48 | – |
| 0190-0x | Gruppe 1 | 0,15 | – | 0,03 | – |
| 0190-0x | Gruppe 2 | 0,25 | – | 0,13 | – |
| 0190-0x | Gruppe 3 | 0,12 | 0,51 | – | 0,41 |
| 0190-0x | Gruppe 4 | 0,12 | 0,77 | – | 0,61 |
| 0190-0x | Gruppe 5 | 0,12 | 1,28 | – | 1,02 |
| 0190-0x | Gruppe 6 | 0,12 | 2,05 | – | 1,63 |

**Angaben:** Deutsche Telekom, Stand 4. 1. 2002. Alle Tarife inkl. 16% Umsatzsteuer.

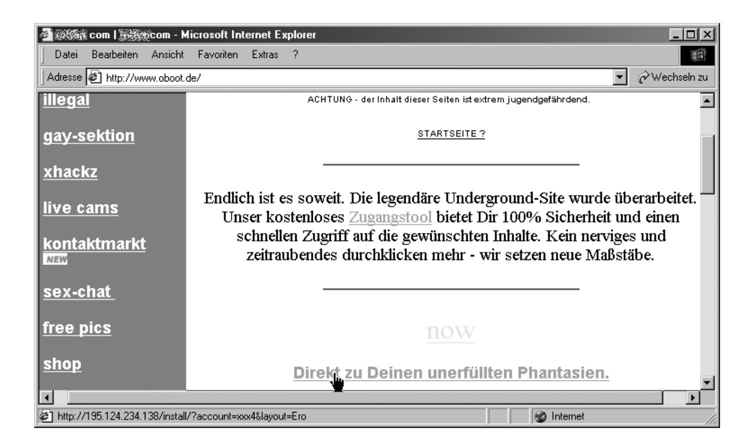
Ab 2004 werden die bisherigen 0190-Nummern von Vorwahlen abgelöst, die mit 0900 beginnen. Die neuen Nummern vergibt die Regulierungsbehörde nicht mehr in Tausenderblöcken an die Netzbetreiber, sondern einzeln an die Inhalte-Anbieter. Diese können die Preise frei gestalten: Für Premium-Dienste, die über eine 0900-Einwahl laufen, gibt es keine Tarifgruppen.

## 3.4.10 0190-Dialer: Tricks der Anbieter

Wer per DSL surft und keine zusätzliche Modem- oder ISDN-Karte als Backup im Rechner stecken hat, ist durch 0190-Dialer nicht gefährdet: Ein eingeschaltetes DSL-Modem ist permanent mit dem Netzwerk des Providers verbunden, eine Einwahl ist somit nicht erforderlich. Beim Verbindungsaufbau übermittelt Ihr Rechner nur Ihre Kennung und das Passwort, um sich zu authentifizieren.

Aufpassen müssen hingegen alle, die sich mit Windows ins Internet einwählen. Wie hoch das Risiko ist, sich einen Dialer einzufangen, hängt eng mit dem persönlichen Surfverhalten zusammen. Anwender, die bedenkenlos auf alle Links klicken, die mit den Begriffen „Gratis“ und „Sex“ werben, haben gute Chancen, die Telefonrechnung in astronomische Höhen zu treiben.

Unseriöse Anbieter versuchen häufig, User mit Hilfe von so genannten Vertipper-Domains anzulocken. Dabei handelt es sich um Internet-Adressen, die denen populärer Sites ähneln und sich nur durch typische Schreibfehler unterscheiden. Wer etwa www.oboot.de statt www.uboot.de aufruft, landet auf einer „legendären Underground-Site“. Dort verheißt ein kostenloses Zugangstool hundertprozentige Sicherheit und einen schnellen Zugriff auf die gewünschten Inhalte. Der Link zu den „unerfüllten Phantasien“ führt schnurstracks zur Installation eines 0190-Dialers.




**Sicher zum 0190-Dialer:** Wer seine „unerfüllten Phantasien" so befriedigen will, zahlt einen hohen Preis.

Viele User versichern jedoch, nie so ein Programm geladen zu haben. Die Software müsste sich somit selbstständig beim Besuch einer Webseite installieren. Die Chance besteht, falls man einen schlecht konfigurierten Browser verwendet, der ActiveX versteht – was zurzeit nur der Internet Explorer beherrscht. In dem Fall lädt ein ActiveX-Control den Dialer und installiert ihn nach einem Neustart auf dem System des Anwenders.

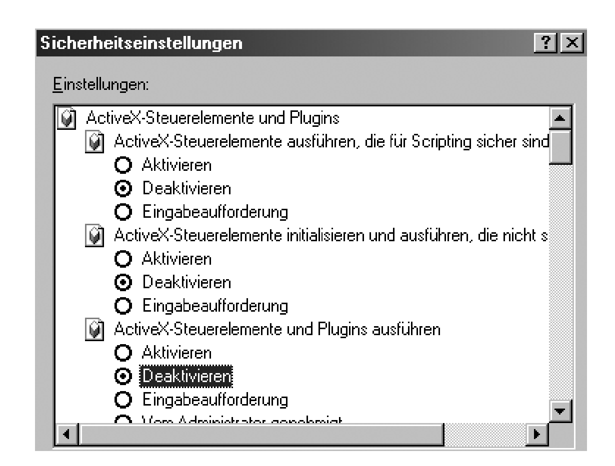
## 3.4.11 0190-Dialer: Schutz

Die rigoroseste und gleichzeitig effektivste Schutzmöglichkeit gegen die Dialer besteht darin, die teuren Vorwahlbereiche beim jeweiligen Netzbetreiber zu sperren. Der verlangt dafür meist eine Gebühr, die bei der Deutschen Telekom einmalig 7,67 Euro beträgt.

Wer eine Telefonanlage besitzt, kann meist darüber die Anwahl festgelegter Rufnummern für bestimmte Nebenstellen verbieten. Sinnvoll ist das auf jeden Fall für den Anschluss, den der PC benutzt.

Bei allen Sperrmaßnahmen sollte man bedenken, dass vermehrt Dialer auftauchen, die nicht eine 0190-Nummer benutzen, sondern die Vorwahlen 0193, 0192 oder 0191. Diese Bereiche sind Service-Providern zugeteilt, die die Kosten pro Online-Minute selbst festlegen können.

Wer nicht gleich Nummern sperren will, kann über die Konfiguration seines Rechners, besonders des Browsers, viel erreichen. Gerade der Internet Explorer macht das Surfen durch die Unterstützung von ActiveX nicht unbedingt sicherer. Daher sollten Sie ActiveX über den Punkt Sicherheit in den Internet-Optionen abschalten. Das verhindert die automatische Installation unerwünschter Dialer auf dem PC durch ActiveX-Controls. Benutzer anderer Browser wie Opera oder Netscape sind hiervon nicht betroffen, zumindest, solange sie die fehlenden ActiveX-Fähigkeiten nicht durch Plug-ins nachgerüstet haben. Im Internet Explorer sollten Sie ebenfalls den automatischen Datei-Download deaktivieren. Diese Einstellung (Extras/Internetoptionen/Stufe anpassen/Dateidownload) verhindert, dass ActiveX -gesteuerte Downloads von Dialern erfolgen.




**Beruhigter surfen:** Wer ActiveX in den Sicherheitseinstellungen des Internet Explorer deaktiviert, gibt automatischen Dialer-Installationen keine Chance.

Tools wie der Web.de SmartSurfer (http://smartsurfer.web.de), die das Windows-DFÜ-Netzwerk auf unerwünschte Dialer überwachen, stellen einen zusätzlichen Schutz dar. Komplett sollte man sich darauf jedoch nicht verlassen. Insbesondere, da einige 0190-Dialer gezielt die Schutzprogramme ausschalten.

## 3.4.12 Fazit

Jeder, der im Internet surft, muss sich darüber im Klaren sein, dass er nicht alleine ist. Millionen anderer User überall auf der Welt sind gleichzeitig online. Genau wie im realen Leben gibt es darunter gesetzestreue Bürger, aber auch zwielichtige Gestalten mit unseriösen Angeboten.

Die schwarzen Schafe versuchen mit einer Kombination aus technischen Angriffen und psychologischen Ansätzen, so genanntem Social Engineering, zum Zuge zu kommen. Diese Taktik lässt sich gut anhand der untergeschobenen 0190-Dialer erkennen.

Als Erstes empfiehlt es sich daher, die Schwachstellen der Standard-Internet-Software – Browser und Mail-Client – auszuräumen. Dazu gehört, Patches für Sicherheitslücken zeitnah zu installieren. Ein regelmäßiger Blick auf die entsprechenden Webseiten des Herstellers ist Pflicht.

Doch es gilt, auch die Standardvorgaben unter die Lupe zu nehmen. So sollten Sie die Ausführung aktiver Inhalte wie JavaScript, VBS und ActiveX nur absolut vertrauenswürdigen Sites gestatten. Das Zonenmodell des Internet Explorer ermöglicht eine abgestufte Sicherheitspolitik.

Die größte Schwachstelle allerdings bleibt der Mensch vor dem Monitor. Noch so ausgeklügelte technische Schutzmaßnahmen können gegen Social-Engineering-Attacken kaum etwas ausrichten. Hier hilft nur, die Anwender gezielt über die Gefahren aufzuklären, damit sie sich mit einer gesunden Portion Misstrauen im Internet bewegen.

Thomas Rieske und Mike Hartmann

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Safer surfen | a395 | – |
| Dem Surfer auf der Spur | a284 | – |
| Sichere E-Mail | a398 | – |
| Internet Underground | a280 | – |
| Virenscanner im Test | a214 | – |
| Test: Sechs Personal Firewalls | a405 | – |

# 4 Katastrophenvorsorge

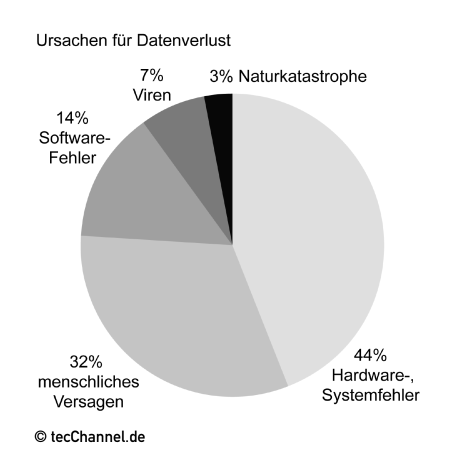
Ein Sicherheitskonzept sollte nicht nur den Schutz vor Viren und Hackern beinhalten. Es muss auch vor Datenverlust schützen und gegebenenfalls einen dauerhaften Betrieb des Netzes und der produktionsrelevanten Server im Auge haben. In diesem Artikel lesen Sie, mit welchen Verfahren Sie sich gegen einen Totalausfall schützen können, wie Sie eine fehlertolerante Infrastruktur aufsetzen und wie so ein Sicherheitskonzept für mittelständische Unternehmen aussehen könnte.

## 4.1 Katastrophenschutz mit Plan

Trotz aller technischen Vorsichtsmaßnahmen und Hilfsmittel lässt sich ein Totalausfall der Datenverarbeitung nicht immer verhindern. Der automatische Ablauf vorbereiteter und erprobter Notfallpläne mindert jedoch die Schäden.

Fällt der Begriff Katastrophe, tauchen vor dem inneren Auge unwillkürlich Bilder von brennenden Gebäuden, überschwemmten Landstrichen oder von Erdbeben geschüttelten Städten auf – die klassischen Naturkatastrophen und Auswirkungen der viel zitierten „höheren Gewalt“. Die Informationstechnik jedoch fasst den Begriff viel schlichter: Einen Katastrophenfall (kurz: K-Fall) stellt hier jede Komplettunterbrechung der Datenverarbeitung dar, aus welchem Grund auch immer.

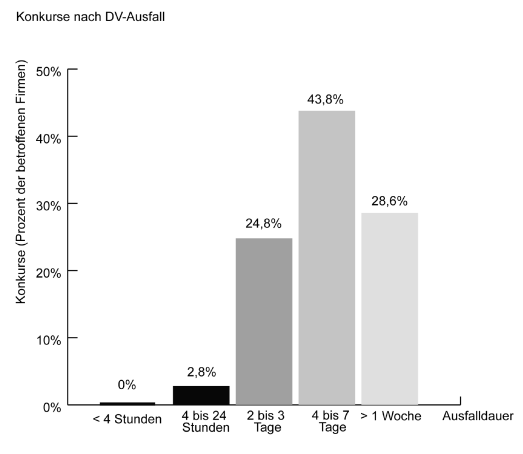
Zu den Ursachen für K-Fälle zählen natürlich Naturkatastrophen wie Überflutungen oder Erdbeben. Sie stellen hier aber die absolute Ausnahme dar. Zusammen mit Bränden und schlichten Wasserschäden machen sie gerade einmal drei Prozent aller totalen Datenverluste aus. Dagegen zeichnen Hardware- und Systemfehler für nahezu die Hälfte aller DV-Katastrophen verantwortlich, ein weiteres Drittel geht auf das Konto menschlichen Versagens.




**Risikofaktor Mensch:** Neben fehlerhafter Hardware verursacht vor allem menschliches Versagen einen Großteil aller katastrophalen Datenverluste.

Dass es sich beim Totalausfall der Rechnerinfrastruktur um mehr als nur eine vorübergehende Unpässlichkeit handelt, belegt schon die durchschnittliche Schadenssumme eines K-Falls: Nach Schätzungen renommierter Analysten liegt sie bei stolzen 900.000 Euro. Diese Summe umfasst wohlgemerkt nur die unmittelbaren Schadens- und Wiederanlaufkosten; mittelbare Kosten, etwa durch Nichterfüllbarkeit oder Nichtzustandekommen von Aufträgen, sind hier noch nicht einkalkuliert.

Dementsprechend drastisch fallen die Folgen aus. Wie eine Studie der Universität von Minnesota belegt, geht rund ein Viertel der von DV-Katastrophen betroffenen Unternehmen unmittelbar in Konkurs, weitere 40 Prozent überleben danach längstens zwei Jahre. Nur sieben Prozent der untersuchten Betriebe schließlich waren fünf Jahre nach dem K-Fall noch auf dem Markt. Dabei hängt die Überlebensfähigkeit des Unternehmens offenbar stark von der Dauer des DV-Ausfalls ab – dies legt jedenfalls eine Untersuchung der Debis Systemhaus nahe.

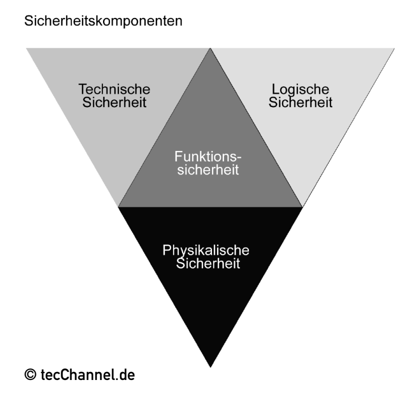



**Todeszone:** Fällt die Unternehmens-DV für mehr als 24 Stunden aus, stellt das die Überlebensfähigkeit der Firma ernsthaft in Frage.

Als relativ ungefährlich erweisen sich danach K-Fälle von maximal 24 Stunden Dauer; nicht einmal drei Prozent der untersuchten Unternehmen scheiterten in diesem Fall. Selbst längere Ausfälle der Datenverarbeitung von bis zu drei Tagen Dauer können viele Unternehmen noch verkraften. Steht die DV jedoch für vier oder mehr Tage, folgt fast unweigerlich das endgültige Aus.

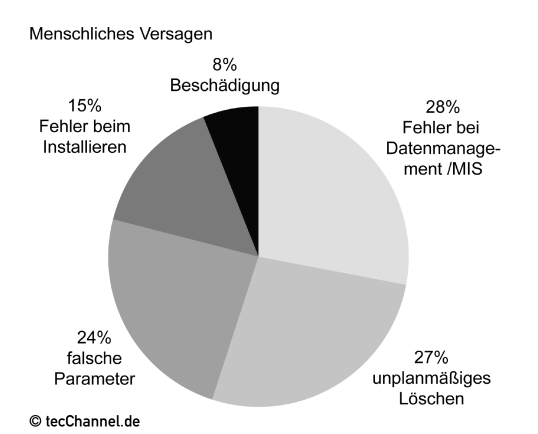
## 4.1.1 Vorbeugung vs. Katastrophenvorsorge

Im Mittelpunkt aller Anstrengung stehen daher Maßnahmen, die dem Katastrophenfall vorbeugen sollen. Dabei gilt es, die Anforderungen der technischen, logischen und physikalischen Sicherheit aufeinander abzustimmen, um eine optimale Funktionssicherheit der DV zu gewährleisten.




**Puzzlespiel Safety:** Ein wirksamer Katastrophenschutz setzt voraus, dass alle Sicherheitsaspekte ausreichend berücksichtigt werden.

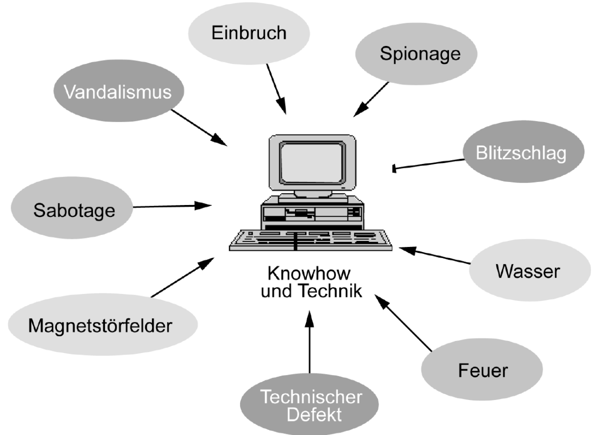
Tatsächlich lassen sich viele der Ursachen für katastrophale Datenverluste schon im Vorfeld durch technisch-organisatorische Maßnahmen auffangen. Redundante Serverkomponenten bis hinunter zur Netzwerkkarte, RAID-basierte Massenspeichersysteme und eine Stromversorgung via USV schalten die klassischen Verursacher von Hardware- und Systemfehlern aus. Leistungsfähige Backup-Software sichert täglich Hunderte Gigabyte an Daten auf schnelle Tape Libraries, ausgefeilte Virenscanner schützen Server und Clients gegen Infektionen aus dem Netz.




**Fatal Error:** Fehlbedienungen durch den Benutzer verursachen mehr als drei Viertel aller katastrophalen Datenverluste.

Nur all zu leicht verleitet der Einsatz dieser perfekten technischen Mittel zu einem falschen Gefühl der Sicherheit. Menschlichem Versagen gegenüber bleibt die Technik völlig machtlos, und auch Faktoren wie Sabotage, Einbruch oder Diebstahl gegenüber reicht ihre Schutzfunktion nicht allzu weit. Hinzu tritt die oft unterschätzte Gefahr durch Brand, Wasserschäden und Blitzschlag.

Katastrophen lassen sich daher weder voraussehen, noch mit letzter Sicherheit vermeiden. Wohl aber können ihre Folgen – bei vorausschauender Planung – in engen Grenzen gehalten werden.

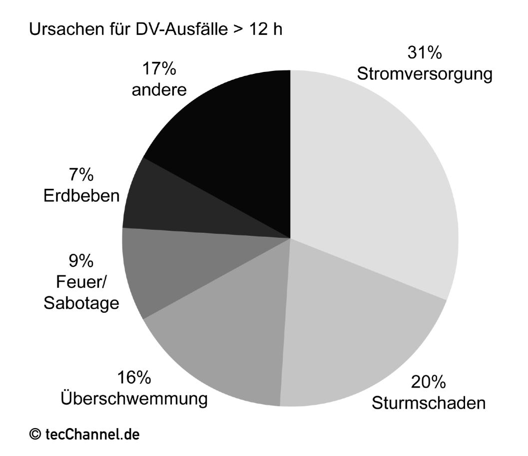



**Zielscheibe Information:** Als Ursache für katastrophalen Datenverlust kommen zahlreiche, durch Technik nur bedingt beherrschbare Einzelfaktoren in Frage.

Ein Beispiel: „Wenn mir das Haus über dem Kopf abbrennt, dann nützt mir mein Backup auch nichts mehr ...", so lautet eine gängige Gegenargumentation zur Konzeption der Katastrophenvorsorge. So überzeugend diese Aussage zunächst klingen mag, sie entbehrt bei näherer Betrachtung jeder Grundlage.

Zum einen vernichtet relativ selten ein Brand ein komplettes Gebäude – so selten, dass ein derartiges Ereignis Fernseh-Nachrichtenwert besitzt. In den allermeisten Fällen betreffen Brände nur einzelne Räume, oft allerdings auf Grund mangelnder Planung mit katastrophalen Folgen: So stehen etwa nach dem Brand eines Serverraums keine Ersatzsysteme parat, auf die sich das Backup aufspielen ließe; meist ist noch nicht einmal deren schnelle Beschaffung vorbereitet. Oder: Da die Backup-Tapes ebenfalls im Serverraum lagerten, wurden sie durch Hitze und korrosive Brandgase unbrauchbar...

Die Liste ließe sich beliebig fortführen. Selbst falls das Firmengebäude nur noch aus rauchenden Trümmern besteht, könnte – wiederum unter Vorliegen eines präparierten Wiederanlaufplans – zumindest ein Notbetrieb in einer anderen Firmenfiliale, bei einem Partnerunternehmen oder in einem Ausweichrechenzentrum eingeleitet werden.




**Quellen der Bedrohung:** Zwei Drittel sämtlicher länger andauernden DV-Ausfälle werden durch Unwetter oder gravierende Unterbrechungen der Stromversorgung verursacht.

## 4.1.2 Vorarbeiten

Als Grundlage zur Erstellung des Katastrophenvorsorgeplans dient eine umfassende Schadenspotenzial-Analyse. Dazu sind zunächst einmal die Schlüsselsysteme und -anwendungen, die das Rückgrat des Unternehmens bilden, zu identifizieren und zu priorisieren.

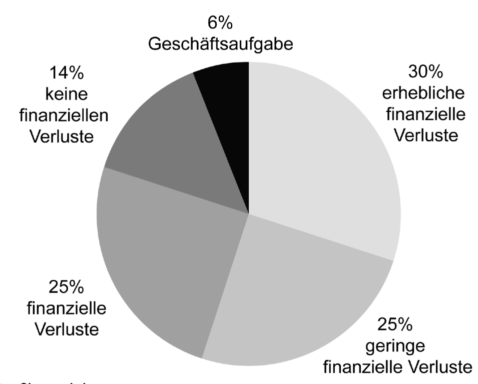
Üblicherweise fasst man dazu diese Komponenten in Form einer Liste zusammen, die Rechner und Anwendung einander zuordnet und eine maximal tolerierbare Ausfallzeit festlegt. Dabei erweist es sich in der Regel als praktikable Vorgehensweise, zu den einzelnen Applikationen den Leiter der verantwortlichen Abteilung nach maximal verträglichen Ausfallzeiten zu befragen.

Neben der nötigen Systemverfügbarkeit gilt es, die Hardware-Voraussetzungen, wie Prozessortyp oder den notwendigen Massenspeicherplatz, zu ermitteln. Zudem muss auch die Abhängigkeit vom Bestehen bestimmter LAN- und WAN-Verbindungen geprüft werden.

Nach der Erfassung aller relevanten Parameter genügt eine schlichte Sortierung dieser Systemliste nach den tolerierbaren Standzeiten, um ein klares Bild über die Wichtigkeit der einzelnen Rechner für das Funktionieren des Unternehmens zu erhalten. Mit Hilfe der Liste lässt sich darüber hinaus auch festlegen, welche internen und externen Ausweichmöglichkeiten beim Ausfall eines bestimmten Rechnersystems bestehen.

Dabei reichen die internen Alternativen von der Verlagerung wichtiger Anwendungen auf gering priorisierte Systeme bis zur Bereithaltung kompletter, vorinstallierter Ersatz-Hardware. Für Applikationen mit geringer Priorität kann es auch genügen, vorab mit dem Hardware-Lieferanten definierte Fristen zur Bereitstellung von Ersatzsystemen zu vereinbaren.






**Teure Daten:** Über die Hälfte aller von Datenverlusten betroffenen Unternehmen müssen schmerzliche finanzielle Verluste hinnehmen. Für jedes Zwanzigste bedeuten verlorene Daten das endgültige Aus.

Lassen sich durch interne Systeme die Verfügbarkeitsanforderungen nicht erfüllen, sollten Sie sich nach externen Ausweichmöglichkeiten umschauen. In größeren Unternehmen mit mehreren Filialen bietet es sich an, bei Bedarf zumindest einen eingeschränkten Betrieb auf Rechnern einer anderen Geschäftsstelle vorzusehen. Aber auch Betriebe mit einem einzelnen Sitz müssen sich nicht zwangsläufig nach einem Ausweichrechenzentrum umsehen: Hier bietet es sich beispielsweise an, mit einem Geschäftspartner Ausweichmöglichkeiten auf Gegenseitigkeit zu vereinbaren.

## 4.1.3 Notfallhandbuch

Nach Abschluss dieser Vorarbeiten können Sie mit der Erstellung eines Notfallhandbuchs beginnen.

Im ersten Abschnitt müssen zunächst einmal die für den Ablauf der Katastrophenschutzmaßnahmen verantwortlichen Personen benannt werden.

Auf Grund des für diese Aufgabe notwendigen großen Entscheidungsspielraums sollte der Leiter des Krisenteams der Geschäftsleitung angehören. Zur Bewältigung der Situation benötigt der Krisenmanager ein Team, das je nach Firmengröße aus vier bis mehreren Dutzend Mitgliedern besteht. In jedem Fall gilt es, folgende Funktionen abzudecken:

- Schadensaufnahme an den betroffenen Systemen
- Auswahl der benötigten Datensicherungsmedien aus dem Backup-Archiv und Transport zur Ausweichlokation
- Bereitstellung und Einrichtung des Ausweichsystems an der vorgesehenen Stelle sowie
- Anbindung der betroffenen Benutzer an den Ausweichrechner.

Dabei erhält jedes Mitglied des Krisenteams eine klar umrissene, schriftlich festgelegte Aufgabe zugewiesen. Diese findet sich, zusammen mit dem Alarmierungsweg für das Teammitglied, im Alarmplan wieder.

Zudem legt der Alarmplan die Anlaufpunkte der einzelnen Funktionsträger fest und enthält auch andere relevante Notrufnummern. Dazu zählen neben Feuerwehr, Polizei und Notarzt in jedem Fall die Notzentralen des zuständigen Wasser- und Stromversorgers, gegebenenfalls auch die Nummern externer Datenträgerarchive oder Ausweichrechenzentren.

Nach dem Alarmierungsplan folgt als zweiter Bestandteil des Notfallhandbuchs eine nach möglichen Störungen gegliederte Liste von Notfallplänen. Vergessen Sie nicht, neben den rein technisch bedingten Ausfallursachen auch die Auswirkungen von Einbrüchen, Vandalismus oder Bombendrohungen zu berücksichtigen. Hier sollte sich für jede zu berücksichtigende Situation ein Katalog von zu ergreifenden Maßnahmen inklusive der Benennung der dafür verantwortlichen Personen finden.

Der dritte und wichtigste Part des Notfallhandbuchs besteht aus den dezidierten Wiederanlaufplänen für jede als wichtig identifizierte DV-Komponente. Er dokumentiert:

- welche internen und externen Ausweichmöglichkeiten zur Verfügung stehen
- wie die entsprechenden Komponenten aufzubauen und gegebenenfalls zu installieren sind
- welche System- und welche Anwendungs-Software aufzuspielen ist
- wo und mit welcher Identifikation sich die entsprechenden Datenträger befinden sowie
- welche Mitglieder des Krisenteams in welcher Aufgabenverteilung für den Wiederanlauf verantwortlich zeichnen.

Ein Dokumentationsteil schließt das Notfallhandbuch ab. Er erfasst für jedes wichtige IT-System:

- einen Ersatzbeschaffungsplan, der die Komponenten mit Bezeichnung, Gerätenummer und Beschaffungsdatum identifiziert. Er führt Hersteller und Lieferant des Systems inklusive Adressen und Telefonnummern auf und beschreibt die voraussichtliche Lieferzeit und Dauer der Reinstallation.
- eine Liste der Lieferantenvereinbarungen inklusive Ersatzteil- und Nachkaufgarantien, zugesicherter Lieferzeiten sowie Support-Dienstleistungen inklusive Hotline-Nummern
- sowie last not least ein Verzeichnis professioneller Datenrettungsdienste für den Fall von unvermutet auftretenden Datenverlusten.

Nach der Fertigstellung des Notfallhandbuchs erhält jedes Mitglied des Krisenteams ein eigenes Exemplar, zudem empfiehlt sich die Verteilung zusätzlicher Kopien auf mehrere, jederzeit frei zugängliche Stellen im Betrieb.

### 4.1.4 Notfallübungen

Die Erstellung des Notfallhandbuchs allein garantiert jedoch noch kein reibungsloses Funktionieren der Alarmierungs- und Notfallpläne. Eine regelmäßige Überprüfung und Ergänzung der gesammelten Angaben wenigstens im Quartalsrhythmus ist unumgänglich.

Das regelmäßige Durchspielen ausgesuchter Schadensszenarien in Form von Notfallübungen erprobt nicht nur den effektiven und reibungslosen Ablauf der Wiederanlaufpläne, sondern deckt in aller Regel gnadenlos vorhandene Mängel auf. Zwar stören solche Übungen den regulären Betriebsablauf; dennoch sollten Sie auf dieses Hilfsmittel zur laufenden Optimierung Ihrer Katastrophenvorsorge nicht verzichten.

Jörg Luther

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Ausfallsichere Systeme | a422 | S.193 |
| Professionelle Datenrettung | a651 | – |
| Sicher durch Biometrie | a824 | – |
| Die Netzwächter | a600 | – |

## 4.2 Ausfallsichere Systeme

Ob öffentliche Webserver, interne Fileserver oder Produktions-PCs, ein Ausfall kostet Geld und Renommee. Dabei kann man einen Rechner schon mit geringen Mitteln gegen Ausfälle sichern.

Mit dem Internet gewinnen Server eine offenkundigere Bedeutung: Der öffentliche Auftritt jedes Unternehmens steht und fällt mit der Verfügbarkeit der Hardware/Software-Kombination. Ausfälle sind peinlich und können in kurzer Zeit beträchtliche Einbußen an Umsatz und Kunden nach sich ziehen. Aber auch der Ausfall firmenintern genutzter Rechner führt zu einem Arbeitsstopp und kann dadurch recht teuer werden. Die Lösung besteht in ausfallgesicherten Systemen. Doch die professionellen Anbieter solcher Systeme verlangen häufig einen Obolus, der manche Firma erblassen lässt. Die Grenze von 50.000 Euro wird schnell durchbrochen.

Für den engagierten Systemverwalter oder Webmaster stellt sich daher die Frage: Geht es, bei nahezu gleicher Sicherheit, nicht auch billiger? Und es geht – selbst aus einem Standard-PC, der als Server arbeiten soll, lässt sich mit etwas Aufwand ein passabel abgesichertes System herstellen. Vorausgesetzt, man kennt die neuralgischen Stellen, die abgesichert werden müssen.

Probleme bereiten Hardware-Defekte, Netzwerk-Ausfälle, Software-Fehler und Angriffe von außen. Dieser Beitrag geht ausschließlich auf die ersten drei Bereiche ein. Kostengünstige RAID-Systeme, ausfallgesicherte Netzteile sowie redundante Netzwerkkarten und Software für eine hohe Verfügbarkeit kommen hierfür als Lösung in Frage. Statistiken zeigen übrigens, dass Netzteile und Festplatten die Hauptursachen für Ausfälle sind. Doch die Absicherung fängt bei sehr einfachen Dingen an.

### 4.2.1 Die kleinen Dinge

Im Bereich der Hardware-Ausfälle zeigen sich immer wieder zwei Ursachen für Fehler verantwortlich: mechanische Defekte und thermische Probleme. Unter mechanischen Defekten kann man neben Kontaktfehlern durch Verschmutzung und Korrosion auch den Verschleiß drehender Teile eines Rechners subsumieren, also Festplatten, CD-ROM-Laufwerke und die zahlreichen Lüfter.

Der ständige Luftstrom durch den Rechner bewirkt den Staubsauger-Effekt: Die eingesaugten Partikel lagern sich auf Kontakten ab und sorgen mit der Zeit für Probleme – insbesondere beim Einbau neuer Komponenten. Gleichzeitig verringert die Verschmutzung die Kühlung von Bauteilen. Bessere Gehäuse haben vor den Lüftungsöffnungen ein Filtervlies, das den Staub abhält. Wichtig ist aber, dieses gelegentlich zu reinigen. Ansonsten kann der verringerte Luftdurchsatz zur Überhitzung im PC führen.

Thermische Probleme hängen meist mit defekten Lüftern zusammen. Neben der Temperaturüberwachung beispielsweise im PC-Innenraum haben sich Lüfter mit Tachoausgang bewährt. Fällt ein Lüfter aus oder wird er langsamer, löst der PC einen Alarm aus. Neben der Überwachung eines Lüfters ist auch dessen Dimensionierung nicht zu vernachlässigen. Anhand der Leistungsaufnahme heutiger Netzteile zeigt sich, dass der Leistungshunger selbst von Desktop-PCs in der Spitze bei über 250 Watt liegen kann, die das Gehäuse auch wieder verlassen müssen. Zu kleine Lüfter, Verschmutzung und ungünstiger Aufbau – beispielsweise durch schlecht verlegte Flachbandkabel und dicht gepackte schnelle Festplatten – lassen Komponenten rapide altern.

Hohe Temperaturen verkürzen die Lebensdauer. Wird ein elektronisches Bauteil statt bei 25 Grad Celsius Umgebungstemperatur bei rund 50 Grad Celsius betrieben, halbiert sich die projektierte Lebensdauer. Erste Defekte treten dann oft schon nach 24 Monaten auf. Auch bei Festplatten ist ein derartiges Verhalten üblich.



**Hermetisch abgeschlossen:** In dem gekühlten und staubdichten Schrank sind die Server sicher aufgehoben.

Gart der Computer bei sommerlichen Temperaturen im eigenen Saft, ist der Ausfall quasi vorprogrammiert. Professionelle Server laufen daher meistens in teuren, klimatisierten Räumen. Für den Unternehmer, der einen derartigen Aufwand scheut, bieten sich neuerdings die patentierten, gekühlten Systeme von ITIS an. Hier laufen die Rechner bei niedrigen Temperaturen, von der Umwelt hermetisch abgeschieden, in einem „PC-Kühlschrank".

### 4.2.2 Günstiges IDE-RAID

Ausfälle von Festplatten sind besonders kritisch, da die Daten auf einer defekten Platte verloren gehen. RAID-Systeme mit redundanter Datenspeicherung auf mehreren Festplatten schützen vor dem Datenverlust. Ein weiterer Vorteil ist die bessere Performance, die durch parallele Schreib- oder Lesevorgänge entsteht. Der Nachteil sind höhere Kosten für Datenträger und spezielle RAID-Controller. Allerdings ist dieser Nachteil gering gemessen am Wiederherstellungsaufwand für einen defekten Datenträger beispielsweise von einem Backup-Band. Dennoch: RAID schützt nicht vor Datenverlusten durch Löschen oder durch Virenbefall!

Der einfachste Fall von RAID ist die Festplatten-Spiegelung oder RAID-1. Hier werden die Daten gleichzeitig auf zwei identische Festplatten geschrieben. RAID-1 stellt trotz des verschwenderischen Umgangs mit Plattenplatz eine verhältnismäßig preiswerte Lösung dar, weil der Aufwand für die Berechnung spezieller Prüfsummen entfällt. Heutzutage gibt es RAID-Controller auch für IDE-Festplatten, wodurch der Preis sehr günstig gehalten werden kann. Hervorzuheben sind Controller der Firma Promise. Beispielsweise ist die ATA/33-Version des Fasttrak RAID-Controller für 219 Euro erhältlich, die ATA/100-Version kostet etwa 100 Euro. Daher sind IDE-RAID-Controller auch für Amateur-Videofilmer und Power-Gamer unter Windows 98 interessant.

Das schnelle IDE-Interface ist sehr empfindlich, was Kabellängen angeht. Insbesondere bei der Verwendung von Wechselrahmen ist Vorsicht angebracht, weil die Übergangskontakte den Transfer erschweren. Im Zweifelsfall sollte man ein Set kaufen, welches für diese Anwendungen getestet wurde.

Die Performance bei Schreibvorgängen bleibt bei RAID-1 gleich, da die Daten parallel auf beide Platten geschrieben werden. Beim Lesen, wenn die Hälfte der Daten von der ersten, die andere Hälfte gleichzeitig von der zweiten Platte angefordert werden, verbessert sich die Geschwindigkeit um den Faktor 1,6 bis 1,8.

Bei einer RAID-0-Konfiguration werden die Daten nicht gespiegelt, sondern auf die Platten verteilt. Dann wird ein ähnlicher Leistungsgewinn – auf Kosten der Datensicherheit – auch beim Schreiben erreicht. Messungen hierzu finden Sie in unserem Beitrag über Ultra-ATA/100 (**webcode: a453**). Dort stieg beispielsweise der maximale Datendurchsatz einer IBM Deskstar 75 GXP im RAID-0-Verband aus zwei Platten von 36 auf 72 MByte/s an. Die Praxiswerte beim Lesen erhöhten sich von 13,5 MByte/s auf 20,9 MByte/s.

Die Promise-Controller erlauben den Anschluss von vier IDE-Platten, wobei dann RAID 10 (sprich RAID Eins-Null) zum Einsatz kommt. Mit diesem Verfahren werden die Daten gleichzeitig als so genannte Stripes (Streifen) auf die Platten verteilt und anschließend gespiegelt. Die Verteilung auf die Platten führt zu einem großen Leistungsgewinn bei gleichzeitiger Datensicherheit.

## 4.2.3 SCSI-RAID

Im Profi-Bereich hat SCSI trotz aller Totsagungen vergangener Jahre die Nase vorn. Auch hier gibt es RAID-1-Lösungen für ein Plattenspiegelpaar, allerdings kosten diese Lösungen auch deutlich mehr: Sowohl Controller wie auch Festplatten sind teurer. Hervorzuheben sind hierbei die Adaptec 2100- und 2110-Serien, die bei Preisen ab 500 Euro aber auch mehr Funktionen beherrschen als die einfache Plattenspiegelung. Andere Hersteller wie ICP-Vortex verlangen rund 1500 Euro und mehr für die Controller.

Mit mindestens drei Platten lässt sich mit diesen Controllern auch ein RAID-5-System aufbauen. Der Unterschied ist die Berechnung der Redundanz: Hier werden die Informationen durch eine Prüfsumme abgesichert, aus der sich die Daten im Fehlerfall einer Festplatte sicher wieder zurückrechnen lassen. Durch dieses Verfahren lässt sich Plattenplatz sparen, da in der Kapazitätsbilanz immer nur eine Platte die Fehlerinformationen tragen muss. Bei einem System mit 5 x 36 GByte Plattenplatz sind also netto 4 x 36 GByte Platz vorhanden. Die Prüfsummen werden gleichmäßig auf alle Platten verteilt, um die Ausfallchancen zu minimieren.

Der Nachteil von RAID-5 ist der Rechenaufwand: Mit dem schnellen Errechnen der Prüfsummen ist ein ausgewachsener RISC-Prozessor voll beschäftigt. Dies ist auch der Grund, warum solche Systeme nicht ganz billig sind. Bei großen Datenvolumen liegen sie aber ohne Zweifel im Vorteil.

## 4.2.4 SCSI-RAID mit IDE-Platten

Eine interessante Variante sind die externen Standgehäuse oder 19-Zoll-Varianten wie der Brownie AD-600. Hier ist der RAID-Controller in einem externen Gehäuse untergebracht, welches insbesondere für die Bedürfnisse der Festplatten nach guter Kühlung und stabilem Einbau ausgelegt ist. Im Inneren arbeiten kostengünstige IDE-Festplatten. Zum Rechner hin verhält sich dieses externe RAID-System wie eine große SCSI-Festplatte, der Rechner benötigt also keine speziellen RAID-Treiber, sondern nur einen SCSI-Controller. Diese Subsysteme sind auch hinsichtlich Netzteil ausfallsicher gestaltet, laufen stabil und zuverlässig. Nachteilig ist das inzwischen veraltete UltraWide-SCSI-Interface, das lediglich 40 MByte/s übertragen kann. Dadurch ist ein Brownie-RAID langsamer als eine schnelle SCSI-Festplatte. (**webcode: a435**). Auch das intern eingesetzte UDMA/33-Interface entspricht nicht mehr dem aktuellen Standard.

Ein wichtiger Praxisaspekt ist die so genannte Hot-Swap- und Hot-Spare-Funktionalität: Fällt eine Festplatte aus, will man ja nicht stundenlang den Rechner herunterfahren, bis die neue Platte eingebaut und im RAID angemeldet ist. Bei Hot Swap kann die Festplatte deswegen im laufenden Betrieb getauscht werden. Wenn der Controller eine entsprechende Unterstützung bereithält, kann auch der Rebuild-Vorgang nach dem Tausch einer defekten Platte im Laufbetrieb durchgeführt werden. Externe Systeme sind hier wiederum im Vorteil, weil das Betriebs-

system nichts von einem Hot Swap mitbekommt. Im Fall der Brownies ist es außerdem möglich, eine Platte als Hot Spare mitlaufen zu lassen. Diese Platte wird nicht mit Daten befüllt, springt aber sofort ein, wenn eine andere Platte ausfällt. Der Rebuild-Vorgang startet dabei automatisch, ohne dass ein Administrator auch nur einen Finger rühren muss.

### 4.2.5 Software-RAID mit Windows NT, 2000 und XP

Windows NT, 2000 und XP ermöglichen es, Software-seitig mehrere Festplatten zu einer RAID-Partition zusammenzufassen. Die schnellen Stripesets (RAID-0) bieten sowohl die Workstation- als auch die Serverversion, die erhöhte Datensicherheit durch Spiegelung (RAID-1) nur der Server.

Problematisch bei der Software-Lösung ist, dass das RAID erst arbeiten kann, wenn das Betriebssystem gestartet ist. Die Systempartition lässt sich damit also nicht absichern. Als Aufbau empfiehlt sich eine kleine Festplatte, auf der nur das Betriebssystem liegt. Für dieses sollte ein schnell erreichbares Backup existieren. Bewährt hat sich hier ein direktes Image auf einer CD-R, mit der ein Restore auf eine neue Bootplatte in wenigen Minuten möglich ist. Das Image muss aber nach jeder Änderung am System neu erstellt werden.

Für die Daten und Programme kommen zwei möglichst gleich große Platten zum Einsatz. Ist eine Platte größer, geht der überschüssige Platz verloren. Durch die Spiegelung sind die Daten ebenso sicher wie auf einem Hardware-RAID untergebracht. Beim Schreiben ist ein Software-RAID-1 immer langsamer als eine einzelne Platte. Das Betriebssystem muss die Daten doppelt senden und auf beiden Platten ablegen. Anders beim Lesen: Hier werden die Daten abwechselnd von den Platten angefordert. Solange weder Controller noch CPU zum Flaschenhals werden, kann sich so der Datendurchsatz fast verdoppeln.

### 4.2.6 Fazit: RAID

Die Absicherung der Festplatten mittels RAID -Controller ist praktisch ein Muss, um den Rechner ausfallsicher zu machen. Ob man mit der kleinen Lösung eines Spiegelpaars oder mit einem größeren RAID-5-System liebäugelt, ist letztlich eine Frage des Budgets. SCSI ist für Profi-Systeme vorzuziehen, wobei IDE-SCSI-Umsetzer eine interessante Alternative darstellen: Die Platten sind günstig, die Verbindungswege kurz, die Zuverlässigkeit sehr hoch. Empfehlenswert, weil unabhängig, sind die externen, spezialisierten Brownie-RAID-Systeme, die allerdings mit 2500 Euro ohne Festplatten zu Buche schlagen. Software-RAID bietet keinen absoluten Schutz, da die Systempartition nicht abgesichert wird. Dafür ist es, bis auf den zusätzlich nötigen Festplattenplatz, kostenlos.

### 4.2.7 Absicherung des Netzwerks

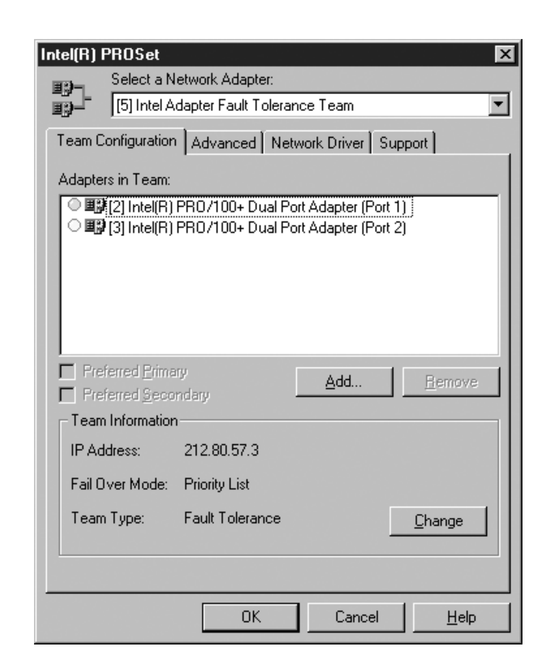
Das Thema Netzwerk und Ausfallsicherheit ist naturgemäß heikel. Oftmals sind einzelne Netzwerkkarten in den Rechnern und Servern eingebaut. Sollte diese Komponente ausfallen, ist das Netzwerk nicht mehr verfügbar. Auch die zumeist unbeachteten Hubs und Switches sind oftmals nur einmal vorhanden. Und, last not least, ist auch die Internet-Anbindung selbst häufig ein so genannter „Single Point of Failure". Eine weitere Einschränkung betrifft die heute übliche Anbindung von Servern: Oftmals verfügen die Geräte nur über eine 100-Mbit-Netzwerkkarte, die ebenso schnell ist wie die eines einzigen Client. Greifen mehrere User gleichzeitig auf den Server zu, wird die Serveranbindung zum Flaschenhals. Mit etwas Überlegung und einigen Handgriffen lässt sich dieser Zustand bedeutend verbessern.

Eine mögliche Lösung ist die Einteilung des Netzwerkes in Subnetze, wobei der Server entsprechend viele Netzwerkkarten wie Subnetze erhält. So ist die Last einerseits besser verteilt, andererseits ist beim Ausfall einer Netzwerkkarte nur das jeweilige Segment vom Netz abgehängt. Die Kosten für diese einfachste Lösung sind gering. Für erhöhte Sicherheit sollten auch auf der Router/Switch-Seite für jedes Subnetz unabhängige Geräte vorhanden sein. Dies erhöht den finanziellen Aufwand deutlich.

Eine weitere, elegante Lösung ist der Einbau von Dualport-Netzwerkkarten oder Netzwerkkarten, die einen speziellen Treiber zur Bündelung von Netzwerkverbindungen (Adapter Teaming) mitbringen. Damit lassen sich gleich zwei Fliegen mit einer Klappe schlagen: Die Karten werden alle unter einer IP-Adresse angesprochen – deshalb ist es nach Außen nicht ersichtlich, welche der Karten die Anfrage entgegennimmt oder Daten sendet. Wenn eine Karte ausfällt, übernimmt die zweite Karte deren Datenpakete, ohne dass ein Client etwas davon bemerkt. Bedingung ist freilich, dass der Treiber für das jeweilige Betriebssystem auch vorliegt.

### 4.2.8 Schneller und sicherer durch Teaming

Durch das Teaming von Netzwerkkarten lässt sich ein guter Leistungszuwachs in Senderichtung, also vom Server zu den Clients erzielen. Beide Adapter können gleichzeitig Daten verschicken, die dann ein Switch an die Clients transferiert. So kann man den vorher beschriebenen Flaschenhals bei der Anbindung von Servern verkleinern, ohne dass etwa eine neue Verkabelung notwendig wird. Beim Empfang funktioniert die Beschleunigung durch diese Kanalbündelung jedoch nur, wenn der Switch mitspielt und weiß, dass er diese IP-Adresse an zwei verschiedenen Ports ansprechen kann.




**Netzwerkkarten im Team:** Mit diesem Treiber können bis zu vier Netzwerkkarten zu einem Team zusammengefügt und unter einer einzigen IP-Adresse angesprochen werden.

Ein gutes Beispiel für Mehrport-Karten sind die Server-Netzwerkkarten von Intel (www.intel.com). Die Karten sind unter der Typenbezeichnung Intel Ether Express PRO 100+ Server Adapter und Intel Ether Express PRO 100+ Dual Port erhältlich. Die erste Baureihe enthält nur einen Ethernet-Chip und muss daher mindestens zwei Mal im Rechner eingebaut werden. Jede Karte belegt wie üblich einen IRQ. Der Dualport-Adapter belegt hingegen nur einen IRQ und auch nur einen Steckplatz, was in dicht gepackten Serversystemen ein großer Vorteil sein kann. Diese Karte verfügt ebenfalls über zwei Ethernet-Chips, jedoch nur eine einzige PCI-Bridge.

Fazit Netzwerk: Ein Netzwerk ausfallsicher zu machen, ist etwas schwieriger, denn es sind gute Kenntnisse hinsichtlich Routing und Subnetz-Architekturen erforderlich. Nur zwei Netzwerkkarten in den Rechner zu stecken, um damit eine Sicherheit zu bekommen, genügt nicht.

## 4.2.9 Redundante Netzteile

Der Stromversorgung wird oft nicht die Aufmerksamkeit geschenkt, die ihr gebührt, denn schließlich hängt von „Saft“ die gesamte Funktion des Rechners ab. Es ist jedoch nicht schwer, für mehr Sicherheit in diesem Bereich zu sorgen.

Netzteile gehören zu den häufigen Ausfallkandidaten. Die Schaltnetzteile müssen eine ernorme Leistung auf verhältnismäßig kleinem Raum umsetzen. Spannungs-

schwankungen und Spitzenspannungen aus dem selten sinusförmigen Netz kommen hinzu und stressen die Schalttransistoren. Weiterhin spielen thermische Probleme eine wichtige Rolle. Nach einem Jahr Betrieb belegt eine dicke Staubschicht einige Komponenten im Netzteil und erhöht dadurch die thermische Belastung.

Eine gute Lösung bei netzteilrelevanten Problemen ist der Einsatz von redundanten Netzteilen. Diese bestehen aus einer passiven Stromverteilung sowie zwei oder drei Einschüben mit den aktiven, spannungsregelnden Komponenten. Wie bei anderen ausfallsicheren Systemen ist ein einziger Einschub in der Lage, den Strom für den Server zu liefern, vorausgesetzt, man dimensioniert die Sache entsprechend. Im Normalbetrieb arbeiten beide Netzteile gemeinsam, wodurch die Belastung der einzelnen Bauteile reduziert wird.

Typisch handelt es sich um 2x250- oder 2x300-Watt-Netzteile, die genügend Leistungsreserven besitzen. Ein eingebauter Summer sowie eine Leuchtdiode informieren den Nutzer über den Ausfall eines Netzteil-Einschubs. Erhältlich sind die Netzteile beispielsweise von Enermax und ElanVital. Redundante Netzteile mit hoher Leistung, die von den Abmessungen und Anschlüssen normalen ATX-Netzteilen entsprechen, haben ihren Preis: Zwischen 300 und 750 Euro kosten die ausfallsicheren Kraftwerke.

## 4.2.10 Weitere Absicherungen

Eine weitere Komponente der Energiezufuhr steht noch vor dem Netzteil: Mit einer unterbrechungsfreien Stromversorgung (USV) lassen sich oftmals mehrere Fliegen mit einer Klappe schlagen. Einerseits ist im Fall des Stromausfalls für eine gewisse Zeit noch Saft für den Rechner da. Anderseits fungieren bessere USVs auch als Netzfilter und leiten Störungen ab. Sie erleichtern damit den Netzteilen die Arbeit fernab der Stressgrenzen der Schalttransistoren. Eine USV gehört also zu einem ausfallgesicherten Server wie eine RAID-Lösung im Festplattenbereich.

Bei der Dimensionierung der USV sind zwei Parameter entscheidend: Die Ausgangsleistung und die Überbrückungszeit. Bei der Ausgangsleistung sollte man nicht nur den Server selbst berücksichtigen. Ist manuelles Eingreifen zum geregelten Herunterfahren nötig, muss auch der Monitor mitversorgt werden. Um den Netzwerkbetrieb aufrecht zu erhalten, benötigen auch die Switches und Hubs eine Notversorgung. In fensterlosen Serverräumen ist ebenfalls eine Notbeleuchtung recht nützlich.

Die Überbrückungszeit legt man typisch auf 15 Minuten aus. Dies reicht aus, um hausinterne Störungen (Sicherung) zu beheben. Professionelle USVs teilen dem Rechner über ein serielles Interface den aktuellen Zustand mit. Dadurch kann zum einen bei Stromausfall eine Meldung an den Administrator verschickt werden. Zum anderen informiert die USV den Server kurz vor der vollständigen Entladung, so dass sich dieser selbstständig kontrolliert herunterfahren kann.

Die restlichen PC-Komponenten sind im Serverbetrieb schwerlich redundant auszulegen: Eine doppelte Grafikkarte ist nicht zwingend sinnvoll, da sie im Servereinsatz eine untergeordnete Rolle spielt. Außer bei hochpreisigen Systemen schützen Mehrprozessor-Lösungen auch nicht vor dem Ausfall bei einer defekten CPU. Sowohl Hardware-Störungen auf dem gemeinsamen Bus als auch der Ausfall von Betriebssystem-Threads bringen den PC mit hoher Sicherheit aus dem Tritt.

Sinnvoll ist auf jeden Fall aber die Absicherung des Systemspeichers durch Fehlerkorrekturbits (ECC). Vorteilhaft sind Rechner, die hierfür Standard-DIMMs verwenden. Proprietäre Bauformen, wie sie beispielsweise Compaq verwendet, kosten mehr als das Doppelte pro Megabyte. Auf der Hauptplatinenebene ist ein Ausfall verheerend, durch redundante Komponenten aber nicht abzusichern. Es gibt jedoch einen Weg, wie trotzdem der Totalausfall einer Anwendung vermieden werden kann.

## 4.2.11 Absicherung durch Backup-Server

Die Aufgabe eines Webservers ist ein 24-Stunden-Job, der auch von Wartungsarbeiten nicht unterbrochen werden sollte. Allerdings brauchen Server Pflege, insbesondere die Bauteile, welche einem mechanischen Verschleiß unterliegen. Gerade Festplatten sollte man im Webbereich nach einer Laufzeit von zwei bis drei Jahren austauschen, bevor die Defekte auftreten. Doch wenn der Server hierzu heruntergefahren wird, muss ein anderer Server einspringen, denn die Internet-Präsenz darf keinesfalls offline sein.

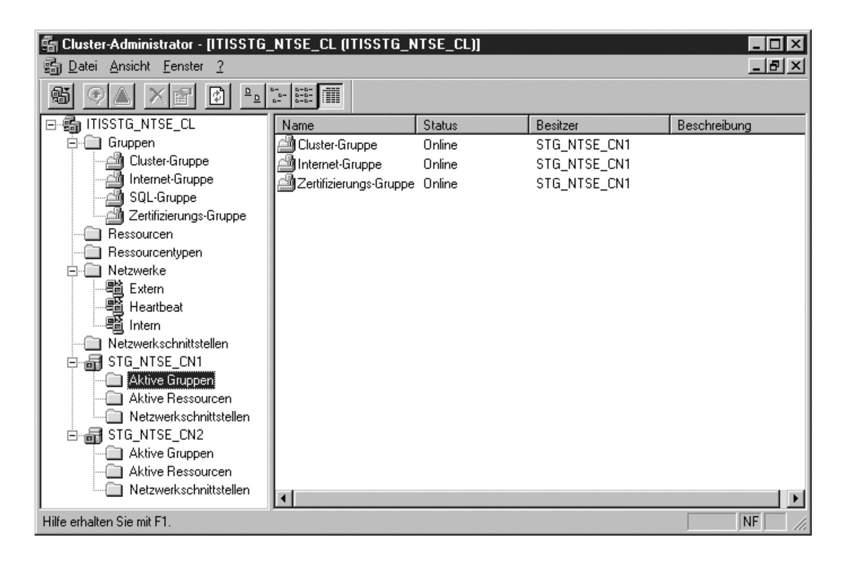
Das einfachste Verfahren ist, einen zweiten Backup-Server aufzustellen, der die gleichen Daten wie der erste Server enthält. Durch Ummappen der DNS-Einträge wird dieser Backup-Server als primärer Server angesprochen, und der Hauptserver kann zu Wartungsarbeiten heruntergefahren werden. Der Nachteil ist allerdings, dass dieses Verfahren einen quasi nutzlos herumstehenden Backup-Server erfordert – schließlich steht dieses Gerät während der Backup-Zeit nicht für andere Aufgaben zur Verfügung.

Der zweite Nachteil ist die Synchronisation der Daten: Da die Dateien während der Laufzeit des Hauptservers übertragen werden müssen, diese Replikation aber einige Zeit in Anspruch nimmt, kann es zu Inkonsistenz kommen. So gehen Bestellungen verloren, wenn sie eingehen, nachdem die entsprechende Logdatei vom Hauptserver kopiert wurde und bevor der Backup die Arbeit aufnimmt. Bei der Rückübertragung auf den Hauptserver entstehen die gleichen Probleme erneut. Die einzige Chance, dies zu vermeiden ist, die Website zumindest während des Kopierens zu stoppen.

## 4.2.12 Cluster-Lösungen und Cluster-Software

Um diese Schwierigkeiten zu vermeiden, gibt es eine Reihe von Hochverfügbarkeitslösungen, die einen dauerhaften Betrieb der Webseiten erlauben, ohne dem Betreiber Probleme mit der Synchronisation aufzubürden. Exemplarisch sei hier die Cluster-Lösung von Windows NT Server Enterprise Edition und Windows 2000 Advanced Server vorgestellt. Ähnliche Lösungen existieren für Unix und Red Hat Linux. Bei Clustern arbeiten mehrere autonome Serversysteme mit einem gemeinsam genutzten Datenträger zusammen. Alle Server haben unterschiedliche Aufgaben; es können auch völlig unterschiedliche Programme auf den Knoten des Clusters laufen.

Im Wartungsfall oder Ausfall eines Serverknotens übernimmt der eine verbleibende Serverknoten ohne Verzögerung die Aufgaben des anderen, inaktiven Knotens einschließlich aller darauf laufenden Applikationen. Voraussetzung ist, dass die Daten auf einem gemeinsam erreichbaren Datenträger liegen, so dass jeder Knoten darauf zugreifen kann.




**Der Cluster-Server im Einsatz:** Die Gruppen lassen sich einzeln auf die beiden Cluster-Knoten verschieben und stellen damit einen lückenlosen Betrieb sicher.

Doch mit dem Cluster-Server lassen sich noch weitere nützliche Szenarien einrichten: Die Cluster-Schicht bildet gegenüber dem Betriebssystem eine Abstraktionsebene für eine Reihe von Ressourcen. Das heißt im Klartext: Auch während des laufenden Betriebs ist eine Zuordnung oder Wegnahme zum Beispiel von IP-Adressen, Servernamen oder kompletten Datenträgern möglich. Dienste und Ap-

plikationen können zum Lastausgleich auf den anderen Cluster-Knoten verschoben werden, während der Server läuft. Dies erhöht die Verfügbarkeit erheblich und erleichtert zudem die Administration.

Doch wo Licht ist, gibt es auch Schatten: Die Einrichtung eines Clusters ist beileibe kein Kinderspiel und kann auch einen erfahrenen DV-Fachmann viel Zeit und Mühe kosten. Günstigerweise greift man hier zu vorkonfigurierten Systemen, die auch im Zusammenspiel mit der Hardware ausgetestet worden sind. Namhafte große Hersteller wie beispielsweise Dell und HP, aber auch kleinere Firmen wie ITIS bieten solche Systeme an.

## 4.2.13 Fazit

Ob ein Server stabil läuft oder nicht, fängt oftmals bei Kleinigkeiten an. Schmutz aussperren, Wärme abführen und Stromversorgung sichern sind einfache, aber wirkungsvolle Maßnahmen. Als Nächstes sind Massenspeicher und Netzwerkverbindungen an der Reihe, die mit doppelter Belegung gegen Ausfall gesichert werden. Für den professionellen Einsatz bieten sich Hardware-Software-Kombinationen mit mehreren Rechnern im Cluster-Betrieb an, wodurch man einen lückenlosen Betrieb gewährleisten kann.

Nach oben hin sind preislich kaum Grenzen gesetzt, doch mit etwas Umsicht lässt sich auch mit preiswerten Komponenten ein sehr stabiles System aufbauen. Doch der gute Murphy kennt keine Gnade, aus diesem Grund gilt: Vergessen Sie nicht das regelmäßige Backup!

Konrad Kraft

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Test: RAID für Workstations | a519 | – |
| RAID im Überblick | a708 | – |

## 4.3 Sicherheitsbewusstsein im Mittelstand

Im betrieblichen Alltag der Unternehmen nimmt der Einsatz von Technologien der Informationstechnik stetig zu. Die schnelle Auftragsabwicklung, eine wirtschaftliche Lagerhaltung und ein effektiver Informationsaustausch innerhalb des Unternehmens oder mit Partnern zählen zu den notwendigen Faktoren für eine wirtschaftliche Produktionsweise.

Vielfach steuern IT-Systeme nicht nur die Produktion, sondern sind zudem auch für haustechnische (Telefon-, Klima- und Heizungsanlagen) sowie sicherheitstechnische Anlagen (Brandmelde- und Überwachungsanlagen) verantwortlich. Jedoch ist das Bewusstsein über die eigene Abhängigkeit von IT-Systemen und die daraus resultierende Verletzlichkeit nicht ausreichend vorhanden.

Die Sicherheit von unternehmenskritischen Daten, geistigem Eigentum wie Konstruktionszeichnungen oder Patenten und Kundendaten sehen noch immer viele als Phänomen an. Beim potenziellen Risiko eines elektronischen Angriffes mangelt es vielerorts noch an der notwendigen Sensibilität.

Denn Informationen als eigentlicher Vermögenswert eines Unternehmens werden immer noch zu wenig erkannt. Jede Kompromittierung der Vertrauenswürdigkeit oder Integrität könnte dabei den Verlust des Kundenvertrauens oder eines Wettbewerbsvorteils nach sich ziehen.

Sicherheitsaspekte für mittelständische Unternehmen umfassen dabei insbesondere die Anbindung an öffentliche Netze (Internet), die Sicherheit des lokalen Netzes sowie die Anwendungssicherheit.

Generell bedingt die Informationssicherheit dabei Maßnahmen, um die Authentizität, Vertraulichkeit, Integrität und Verbindlichkeit von Nachrichten und Informationen sowie die Verfügbarkeit und die berechtigte Benutzung von betrieblichen Ressourcen sicherzustellen.

### 4.3.1 Aspekte der IT-Sicherheit

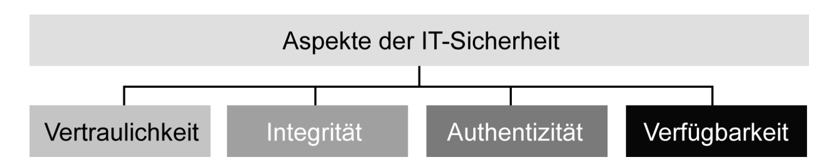
Mit der zunehmenden Vernetzung innerhalb und außerhalb der Firmen droht die Gefahr, dass sich Unberechtigte Zugang zu Informationen verschaffen und Manipulationen vornehmen, um den Unternehmen zu schaden oder sich einen eigenen Vorteil zu verschaffen.

Die Abschätzung dieses Gefahrenpotenzials macht es notwendig abzuklären, gegen wen man sich schützen will. Zum Beispiel kann für eine Organisation das Gefahrenpotenzial aus der Gruppe der Personen in folgende verschiedene Kategorien eingeteilt werden:

- verärgerte ehemalige Mitarbeiter
- unehrliche Mitarbeiter
- Mitarbeiter mit schlechter Schulung

- Hacker oder
- Mitbewerber.

Bei dieser Einteilung ist zu beachten, dass diese Gruppen die Sicherheitsvorkehrungen zum Teil bewusst, teils aber auch unbewusst untergraben. Mehrere Studien belegen, dass sicherheitsgefährdende Vorfälle in Unternehmen zu 60 bis 80 Prozent aus den eigenen Reihen erfolgen.




**Aspekte der IT-Sicherheit:** Ein Sicherheitskonzept in Unternehmen muss die vier Kategorien von Vertraulichkeit bis Verfügbarkeit erfüllen.

Die vier Kategorien Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit bilden die Kriterien, die ein Sicherheitskonzept für ein Unternehmen erfüllen muss. Es sind Anforderungen an ein Modell, das Maßnahmen bereitstellen muss, um ihre Einhaltung gewährleisten zu können.

Mit Vertraulichkeit ist gemeint, dass zu bearbeitende Daten nur den berechtigten Personen zugänglich sind. Ein Verlust liegt bereits vor, wenn nicht genügend Sorgfalt bezüglich ihrer Geheimhaltung eingehalten wird. In jedem einzelnen Unternehmensbereich muss man mit geeigneten Maßnahmen den Eingriff Unbefugter in interne Datenbestände verhindern.

Das Verhindern einer unberechtigten Änderung der verarbeiteten Daten bezeichnet man als Integrität. Dabei ist gemeint, dass der gewünschte Empfänger genau die Daten einer Nachricht erhält, die der Absender übertragen hat. Dieses Integritätskriterium ist auch innerhalb eines Betriebes zu beachten.

Ein interner Mitarbeiter muss beim Dateiaufruf exakt die Informationen bekommen, die zuletzt so gespeichert wurden. Es besteht die Gefahr, dass Unberechtigte im internen Datenbestand der Firma Manipulationen vornehmen oder Online-Dokumente beim Datentransfer verändern.

Unter der Authentizität von Daten wird verstanden, dass der Empfänger erkennen kann, wer der wirkliche Absender eines Dokumentes ist. Der Absender muss aber auch die Gewissheit haben, dass die gesendeten Daten nur an den beabsichtigten Empfänger gelangen.

Als vierter Aspekt der Sicherheitsanforderungen gilt die Gewährleistung der Verfügbarkeit von IT-Dienstleistungen, IT-Funktionen, Informationen und Daten. Sie sollen jederzeit in voller Funktionalität benutzbar sein.

## 4.3.2 Einteilung mittelständischer Unternehmen

Die kleinen und mittelständischen Firmen haben in Deutschland eine entscheidende volkswirtschaftliche Bedeutung. Viele wirtschaftliche Eckzahlen wie steuerpflichtige Umsätze, Bruttowertschöpfung aller Unternehmen, Beschäftigungszahlen aller Arbeitnehmer oder Ausbildungsplätze tragen zu einem großen Teil diese Betriebe.

Zur Beschreibung der quantitativen Kriterien von mittelständischen Unternehmen kommen die Betriebsgröße, die Beschäftigtenzahl und der Jahresumsatz in Betracht. Auf Grund dieser Richtgrößen werden in Deutschland die Firmen wie folgt eingeteilt:

| Unternehmensgröße | Zahl der Beschäftigten | Jahresumsatz in tausend Euro |
|---|---|---|
| klein | bis 9 | unter 500 |
| mittel | 10 bis 499 | über 500 bis 50.000 |
| groß | über 500 | über 50.000 |

**Kleine und große Unternehmen:** Die Einteilung der Unternehmensgröße richtet sich nach der Zahl der Beschäftigten sowie dem Jahresumsatz.

Tendenziell ist zu bemerken, dass Unternehmen mit zunehmender Größe und strukturellem Aufbau in Sachen Informationssicherheit ein höheres Niveau erreichen. In der Betrachtung gehen wir auf Unternehmen mit bis zu maximal 500 Mitarbeitern ein, da diese Unternehmensgruppe in der Regel ein nicht so ausgeprägtes Sicherheitsbewusstsein entwickelt hat.

## 4.3.3 Gefahrenpotenzial

Bei der Nennung der möglichen Gefahrenpotenziale für mittelständische Unternehmen kann nur eine kleine Auswahl getroffen werden. Die folgende Auflistung erhebt nicht den Anspruch auf Vollständigkeit:

- Jedes mittelständische Unternehmen ist potenziell gefährdet. Nicht nur große Konzerne, sondern auch mittelständische Betriebe verfügen über sensible Informationen oder Kommunikationsbeziehungen. Die Gefahr, ein Opfer von Wirtschaftsspionage zu werden, steigt dabei mit der Zunahme von Beziehungen nach außen, über die Informationen ausgetauscht werden sollen. Zu einer weiteren Erhöhung des Gefahrenpotenzials tragen unter anderem auch solche Entwicklungen bei wie Outsourcing oder die externe Vergabe von Wartungstätigkeiten (Fernwartung).

- Gesamtstrategien in der Informationstechnologie sind in mittelständischen Unternehmen selten vorhanden. Investitionen in Informationstechnik erfolgen meistens nur in erforderlichen Einzelsegmenten. Die Entscheidungen für den Einsatz von neuen Technologien werden für bestimmte Bereiche nach Notwendigkeit getroffen. Solche Investitionen sind zum Beispiel der Einsatz von ERP- oder CRM-Software-Lösungen (Enterprise Resource Planning oder Customer Relationship Management). Diese Anschaffungen erfolgen aber nicht im Rahmen einer gesamten IT-Strategie, sondern nur punktuell.
- In der Regel kauft man bei der Anschaffung von Informationstechnologien keine IT-Sicherheitskonzepte mit ein. Die Investition erfolgt nur zur Lösung von Problemen in einzelnen Bereichen des Unternehmens. Notwendige Planungen und die Bereitstellung von Mitteln für die IT-Sicherheit werden in diesem Zusammenhang nicht mit berücksichtigt.
- Sicherheitsgefahren wachsen mit der Nutzung von Informationstechnologien. Es besteht ein enger Zusammenhang zwischen der Erhöhung des Gefahrenpotenzials und der Intensität der Nutzung von neuen Technologien. In Unternehmen mit einer hohen Nutzung existieren mehr Sicherheitsgefahren, da bereits mehr aufgetretene Sicherheitsvorfälle bekannt sind, als in Unternehmen mit einer geringeren Nutzung. Gleichzeitig ist aber zu bemerken, dass in solchen Unternehmen die Schäden durch Fehler der eigenen Mitarbeiter geringer ausfallen als in mittelständischen Betrieben. Dies ist darin begründet, dass in Firmen mit einer intensiven Nutzung der Informationstechnologie die Qualifizierung der Mitarbeiter besser ist.
- Alle Unternehmensbereiche in mittelständischen Unternehmen sind Sicherheitsgefahren ausgesetzt. Insbesondere die betriebswirtschaftlichen Bereiche (beispielsweise Finanzbuchhaltung, Controlling, Forschung und Entwicklung, Produktion) in einem Unternehmen sind als lohnende Angriffsziele für Wirtschaftsspionage gefährdet.

### 4.3.4 Bewältigung von Sicherheitsgefahren

Mit abnehmender Größe von Unternehmen ist auch der Fähigkeit der Bewältigung von Sicherheitsgefahren eine Grenze gesetzt. In kleinen Unternehmen fehlt meistens eine hinreichende Sicherheitsstrategie.

Mit der Annahme, durch eine tägliche Datensicherung sei die Firma bereits hinreichend vor einem Datenverlust geschützt, wird jede weitere Investition in Sicherheit vernachlässigt. Des Weiteren fehlen den mittelständischen Unternehmen in der Regel eine strategische Planung sowie ausreichend qualifiziertes und sensibilisiertes Personal.

Die großen Schwierigkeiten bei der Bewältigung von Sicherheitsgefahren werden bei den kleinen und mittleren Unternehmen nicht nur durch die geringen personellen, sondern auch durch die niedrigen finanziellen Ressourcen hervorgerufen.

Weitere Punkte der schlechten Bewältigung von Sicherheitsgefahren sind:

- Mangelndes Problembewusstsein auf der unteren Mitarbeiterebene sowie der Unternehmensleitung. Ein Schwachpunkt ist zudem in der fehlenden Sensibilität bei den Mitarbeitern zu sehen. Das Management, welches die Unternehmensstrategie entscheidet, hat oft ebenfalls ein geringes Bewusstsein in Fragen der IT-Sicherheit. Vielerorts herrscht das Problem, dass sich das Management der Problematik von Sicherheitsgefahren verschließt und die eigene Firma für zu uninteressant für etwaige Attacken hält. Viele Unternehmer vertreten den Standpunkt, dass sie keine schützenswerten Informationen besitzen.
- Reaktion mit technischen Mitteln auf eingetretene Schäden. In den meisten Unternehmen wird auf eingetretene Schäden mit technischen Mitteln, wie zum Beispiel Verbesserung des Virenschutzes oder Einsatz einer Firewall reagiert. Bei dieser Vorgehensweise erfolgen die höchsten Investitionen in technische oder bautechnische Maßnahmen. Notwendige Investitionen in organisatorische oder personelle Maßnahmen werden vernachlässigt.
- Sicherheit wird nicht als umfassender Prozess verstanden. In vielen Unternehmen werden Investitionen in Sicherheitsprodukte getätigt, wenn bereits Schwachstellen aufgetreten sind und Maßnahmen getroffen werden müssen. Diese Vorgehensweise ist aber nicht in einem Prozess verankert, der sich in einer kontinuierlichen Auseinandersetzung mit Sicherheitsfragen beschäftigt.
- Mangelnde Unterstützung durch die Unternehmensleitung. Viele Unternehmen führt ein kleiner Personenkreis, welcher sich mit der Problematik IT-Sicherheit wenig oder gar nicht auseinander setzt. Die Kosten für mögliche Schäden von Sicherheitsgefahren und deren Auswirkungen auf das Unternehmen lassen sich schwer ermitteln und werden daher durch die Geschäftsleitung nicht genug beachtet. Den Sicherheitsproblemen schenkt man nicht genügend Aufmerksamkeit, weil eine Einbindung in die Betriebsabläufe schwer möglich ist und die Produktorientierung durch den Unternehmer eine solche Sicht erschwert. Aus zeitlichen und finanziellen Gründen will sich das Management oft nicht auf langfristige Entscheidungen für eine IT-Strategie und die damit verbundene IT-Sicherheit festlegen.
- Finanzielle und personelle Ressourcen. Ressourcenprobleme, vor allem finanzieller und personeller Art, führen in mittelständischen Unternehmen dazu, dass Investitionen nicht langfristig geplant und vorbereitet werden. Sie erfolgen mehr oder weniger sprunghaft und konzentrieren sich auf unbedingt erforderliche Maßnahmen. Die Anstellung von Sicherheitsbeauftragten oder auch die Freistellung von Mitarbeitern für die IT-Sicherheit übersteigt in vielen Firmen die vorhandenen Möglichkeiten und wird nicht vorgenommen.
- Einsatz von externen Dienstleistungsunternehmen. Auf Grund der erwähnten geringen Kapazitäten müssten mittelständische Unternehmen verstärkt auf externe Dienstleister zurückgreifen. Diese Inanspruchnahme scheitert nicht nur an den anfallenden Kosten, sondern auch an starren Denkweisen des Managements, die keinem Dritten Einblick in das Unternehmen geben wollen.

- Fehlende Schulung und Weiterbildung in Fragen der IT-Sicherheit. Durch hohe Arbeitsbelastung der Mitarbeiter in mittelständischen Unternehmen ist der Zeitaufwand für Schulungs- oder Informationsveranstaltungen begrenzt. Die starke Einbindung der Mitarbeiter in den Betriebsalltag lässt dafür wenig Spielraum. Gleichzeitig spielen in diesem Zusammenhang auch die geringen finanziellen Ressourcen eine wichtige Rolle.
- Sicherheit im mittelständischen Betrieb. Großunternehmen verlangen von den mittelständischen Betrieben immer mehr Sensibilität in Sicherheitsfragen. Im Zuge der engeren Anbindung von Zulieferern an den Produktionsprozess von Großunternehmen stellen Letztere steigende Anforderungen an eine umfassende IT-Sicherheitspolitik auch innerhalb mittelständischer Unternehmen. Viele große Konzerne verlangen von ihren Zulieferern zur Sicherung ihrer eigenen sensiblen Daten ein hohes Sicherheitsniveau. Leider ist die Unterstützung seitens der „Großen“ noch nicht ausgeprägt genug.

### 4.3.5 Vorhandene Sicherheitslücken im Mittelstand

Eine genaue Analyse der unterschiedlichen Gefahrenpotenziale hat einen großen Einfluss auf geeignete Strategien für die Gefahrenvorbeugung und -abwehr. Jedes mittelständische Unternehmen muss sich die Frage stellen, woher Bedrohungen kommen können. Folgende Fragen stellen sich hier: Werden die meisten Schäden

- durch die eigenen Mitarbeiter
- durch den bewussten Missbrauch von Informationen oder
- durch Datendiebstahl von Externen verursacht?
- Welche Wirkungen haben Viren oder Trojanische Pferde?
- Wie wirken sich Software-Anomalien oder Software-Defekte aus?

Im Folgenden werden einige der besonders häufig vorkommenden Sicherheitsprobleme in Unternehmen aufgelistet:

- Fehler durch eigene Mitarbeiter. Diese verursachen die meisten Schäden, die wie folgt entstehen: Nichtbefolgung von Vorschriften und Anweisungen, unzureichende Ausbildung, Unachtsamkeit und Überforderung, Unzufriedenheit und mangelnde Motivation oder absichtliches Handeln.
- Social Hacking (Erschleichung von Passwörtern). Die geringe Sensibilisierung der Mitarbeiter in Fragen der IT-Sicherheit macht die so genannten Social-Hacking-Attacken zunehmend erfolgreich. Gerade in mittelständischen Unternehmen lässt sich so an sensible Informationen kommen. Das Verfahren basiert nicht auf komplizierten technischen Verfahren und ist mit einfachen Mitteln möglich. Der Angreifer versucht, über das Telefon oder ein persönliches Gespräch über das Sicherheitsbewusstsein im Mittelstand, an Passwörter oder Zugriffs-Codes zu gelangen. Diese Methode ist in Unternehmen mit einer geringen Sicherheitskultur in den meisten Fällen äußerst erfolgreich.

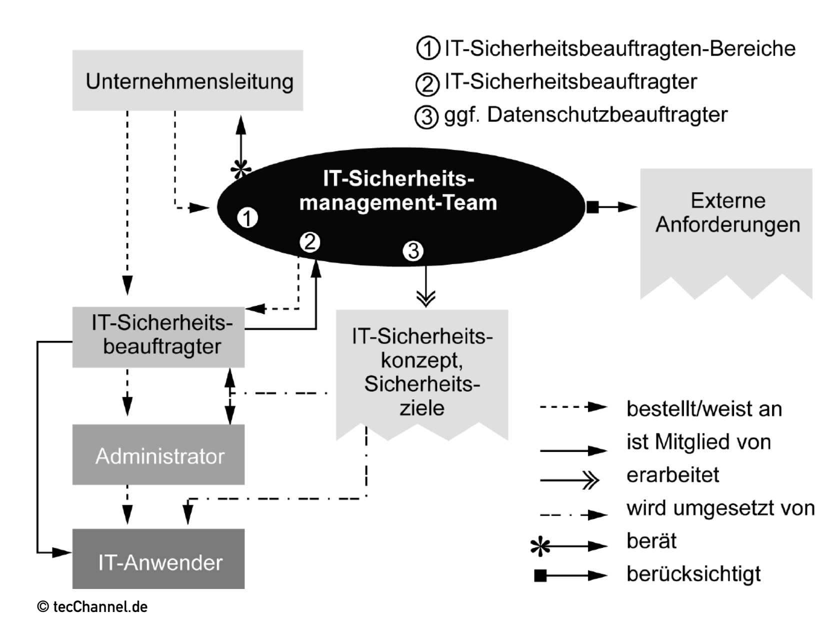
- Einsatz von Firewall-Lösungen. In immer mehr mittelständischen Unternehmen werden Firewalls zum Schutz eingesetzt. Diese entsprechen zum größten Teil den technischen Anforderungen. Diese Lösungen sind allerdings selten in einem umfassenden Sicherheitskonzept integriert, welches ein eigenes Firewall-Konzept verlangt. In dieser Konzeption ist nicht nur der Einsatz einer Firewall beschrieben, sondern auch, dass diese ständig überwacht und aktualisiert werden muss. Nicht selten erfolgen erfolgreiche Angriffe über bekannte Sicherheitslücken in den eingesetzten Firewalls.
- Datenverschlüsselung. Der Datenaustausch mit anderen Unternehmen erfolgt sehr oft über E-Mail. Es wird nicht nur der normale Schriftverkehr über dieses Medium abgewickelt, sondern auch sensible Daten wie Konstruktionszeichnungen, Bilanzen und Angebote werden versendet. Eine Verschlüsselung oder digitale Signaturen sind in den wenigsten Unternehmen etabliert.
- Schulungen im Bereich IT-Sicherheit. Wie oben beschrieben, erfolgen die meisten Schäden durch Fehler der eigenen Unternehmensmitarbeiter. Schulungen zum Thema Sicherheit behandeln jedoch die meisten mittelständischen Betriebe noch immer „stiefmütterlich". Erst bei Sicherheitsvorfällen oder eingetretenen Schäden reagiert man und schickt die Mitarbeiter auf entsprechende Schulungen zum Thema IT-Sicherheit.
- Sicherheitsbeauftragter. Die wenigsten Unternehmen haben die Rolle eines IT-Sicherheitsbeauftragten etabliert. Gerade die Rolle eines Sicherheitsbeauftragten ist jedoch wichtig für die Umsetzung einer umfassenden Sicherheitsstrategie im Unternehmen. Diese Stelle muss jedoch auch mit den entsprechenden Kompetenzen ausgestattet sein, um das Ziel zu erreichen. Dazu gehören etwa Weisungsbefugnisse oder Budget-Verantwortung.

### 4.3.6 Etablierung eines unternehmensweiten IT-Sicherheitsmanagements

IT-Sicherheitsmanagement stellt jenen Teil des allgemeinen Risikomanagements dar, der die Aspekte der IT-Sicherheit wie Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von IT-Systemen gewährleisten soll.

Dabei handelt es sich um einen kontinuierlichen Prozess. Dessen Strategien und Konzepte sind ständig auf ihre Leistungsfähigkeit und ihre Wirksamkeit hin zu überprüfen und bei Bedarf fortzuschreiben. Ebenso wichtig ist eine konsequente Umsetzung der Standards durch sämtliche Mitarbeiter, dazu zählt auch die Geschäftsleitung.

Die angestrebte Sicherheitspolitik sowie die angestrebten IT-Sicherheitsziele kann man jedoch nur erreichen, wenn in einem Unternehmen das IT-Sicherheitsmanagement organisationsweit umgesetzt wird.




**IT-Sicherheitskonzept:** Nur ein komplexes und an das Unternehmen angepasstes Sicherheitskonzept bietet maximale Sicherheit.

Dieser übergreifende Charakter des IT-Sicherheitsmanagements macht es erforderlich, Folgendes innerhalb des Unternehmens festzulegen:

- die IT-Sicherheitsmanagement-Organisation
- die Verantwortlichkeiten
- und die Kommunikationswege.

Zentrale Aufgaben im IT-Sicherheitsmanagement kommen dabei folgenden Instanzen zu:

- dem IT-Sicherheitsmanagement-Team
- dem IT-Sicherheitsbeauftragten des Unternehmens
- bei Bedarf den IT-Sicherheitsbeauftragten der Bereiche
- bei Bedarf den Datenschutzbeauftragten und
- den Administratoren.

Der Aufbau eines unternehmensweiten IT-Sicherheitsmanagements ist notwendig, um einen sicheren Betrieb der Informationstechnologie im Unternehmen zu gewährleisten.

### 4.3.7 IT-Sicherheitsbeauftragter im Unternehmen

Eine Aufgabe des IT-Sicherheitsbeauftragten ist unter anderem, den Mitarbeitern die Bedeutung beziehungsweise die Klassifizierung der Schadenswerte noch eingehender zu vermitteln. So stellt man mit jeder Fortschreibung des Sicherheitskonzepts die Qualität der Ergebnisse sicher. Zu den Pflichten des Sicherheitsbeauftragten gehören:

- die verantwortliche Mitwirkung an der Erstellung des IT-Sicherheitskonzepts
- die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen
- die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen
- die Gewährleistung der IT-Sicherheit im laufenden Betrieb sowie
- die Verwaltung der für IT-Sicherheit zur Verfügung stehenden Ressourcen.

### 4.3.8 Entwicklung eines Sicherheitskonzepts

Ein aufgestelltes unternehmensweites Sicherheitskonzept ist kein statisches, unveränderbares Dokument, sondern muss stets auf seine Wirksamkeit, Aktualität und die Umsetzung in der täglichen Praxis überprüft werden.

Insbesondere ist es von Bedeutung, dass die Liste der existierenden beziehungsweise noch umzusetzenden Sicherheitsmaßnahmen stets dem tatsächlichen aktuellen Stand entspricht. Es ist regelmäßig fortzuschreiben auf Grund

- von Veränderungen technischer Rahmenbedingungen
- von Veränderungen organisatorischer Rahmenbedingungen
- von Veränderungen von Schadenswerten und/oder Häufigkeiten
- des Auftretens neuer Bedrohungen
- des Wegfalls bisheriger Bedrohungen
- und sich dadurch verändernden Risiken
- sowie der Einführung neuer Applikationen.

Ziel muss es sein, das erreichte Sicherheitsniveau zu erhalten beziehungsweise in den kritischen Punkten zu erhöhen. Voraussetzungen für eine effiziente und zielgerichtete Fortschreibung des IT-Sicherheitskonzepts sind:

- die laufende Überprüfung von Akzeptanz und Einhaltung der IT-Sicherheitsmaßnahmen
- die Protokollierung von Schadensereignissen sowie
- die Kontrolle der Wirksamkeit und Angemessenheit der Maßnahmen.

### 4.3.9 Regelmäßige Sicherheits-Audits

Im IT-Sicherheitsprozess geht es nicht nur darum, das angestrebte IT-Sicherheitsniveau zu erreichen, sondern dieses auch dauerhaft zu gewährleisten. Um die bestehende IT-Sicherheitspolitik aufrechtzuerhalten und fortlaufend zu verbessern, überprüft man alle IT-Sicherheitsmaßnahmen regelmäßig. Regelmäßig heißt hierbei aber nicht, dass die Audits an vorhersagbaren Terminen stattfinden, da angekündigte Audits meist ein verzerrtes Bild des Untersuchungsgegenstandes ergeben.

Audits sind vor allen Dingen darauf ausgerichtet, Mängel abzustellen. Für die Akzeptanz von Audits ist es wichtig, dass dies allen Beteiligten als Ziel der Audits erkennbar ist und dass die Audits nicht den Charakter von „Schulmeisterei" haben. Es ist daher sinnvoll, während einer Kontrolle mit den Beteiligten über mögliche Problemlösungen zu sprechen und entsprechende Abhilfen vorzubereiten.

Die Audits können durch externe oder interne Auditoren durchgeführt werden und sollten, so weit möglich, auf standardisierten Tests und Checklisten basieren. Interne Audits werden durch den IT-Sicherheitsbeauftragten durchgeführt. Dieser legt Anzahl, Häufigkeit und Umfang der Audits in Absprache mit dem IT-Sicherheits-Management-Team fest.

Im Rahmen der Audits wird festgestellt, ob die IT-Sicherheitsmaßnahmen auf allen Ebenen im laufenden Betrieb umgesetzt werden. Darüber hinaus übermittelt man mit den Audits, inwieweit die IT-Sicherheitsmaßnahmen bezogen auf die Sicherheitsanforderungen geeignet sind. Zudem wird überprüft, ob die getroffenen Maßnahmen mit den gesetzlichen und betrieblichen Vorgaben übereinstimmen.

Die Ergebnisse werden in einem IT-Sicherheitsreport festgehalten. Dieser sollte auch die vorgeschlagenen Korrekturmaßnahmen aus fachlicher Sicht enthalten.

### 4.3.10 Sensibilisierung des Sicherheitsbewusstseins

Nur durch Verständnis und Motivation ist eine dauerhafte Einhaltung und Umsetzung der Richtlinien und Vorschriften zur IT-Sicherheit zu erreichen. Um das Sicherheitsbewusstsein aller Mitarbeiter zu fördern und den Stellenwert der IT-Sicherheit innerhalb des mittelständischen Unternehmens besonders hervorzuheben, sollte ein umfassendes, organisationsweites Sensibilisierungsprogramm erstellt werden.

Ein solches Programm hat zum Ziel, IT-Sicherheit zu einem integrierten Bestandteil der täglichen Arbeit zu machen. Es ist systemübergreifend zu betrachten. Dabei ist es die Aufgabe eines dafür Verantwortlichen – im Allgemeinen des IT-Sicherheitsbeauftragten – die Anforderungen aus den einzelnen Teilbereichen und systemspezifische Anforderungen hier einfließen zu lassen und dann entsprechend zu koordinieren. Für die Sicherheit des Unternehmens kann man eine Reihe von Maßnahmen nicht technisch erzwingen, sondern man muss sich bei deren Implementierung auf das Mitwirken der Mitarbeiter stützen.

Das Sicherheitsbewusstsein kann durch entsprechende Schulungen beziehungsweise durch Informationen sensibilisiert werden. Dadurch erhöht sich oft auch die Bereitschaft, Unbequemlichkeiten in Kauf zu nehmen, die manche Sicherheitsmaßnahme mit sich bringt. Im Rahmen der Ausbildung beziehungsweise der Einführung neuer Mitarbeiter sollte man daher unbedingt auf das Thema Sicherheit eingehen und den Sinn für potenzielle Bedrohungen schärfen, auch wenn sie noch nicht aufgetreten sind.

Gerade in Bereichen, die über eine perfekte Zugangskontrolle verfügen, gelingt es immer wieder, dass Unberechtigte sich auf Grund von sozialen Verhaltensweisen Zutritt verschaffen. Die Mitarbeiter sind anzuweisen, sich der Berechtigung von Zutrittswilligen stets zu versichern, insbesondere

- unbekanntes Personal, das nicht über eine entsprechende Zugangsberechtigung verfügt, nicht aus falsch verstandener Kollegialität in diese Bereiche zu lassen
- nicht aus falsch verstandener Höflichkeit Unbekannten, die nicht über eine entsprechende Zugangsberechtigung verfügen und sich nicht in Begleitung eines berechtigten Mitarbeiters befinden, den Zugang zu ermöglichen.

Es ist die Entwicklung einer Unternehmenskultur anzustreben, in der Sicherheit, vor allem auch IT-Sicherheit, positiv aufgefasst wird, das heißt als Maßnahme zur langfristigen Sicherung von Arbeitsplätzen und nicht als Behinderung der Arbeit.

Nur so ist eine gewisse Kontrolle der Mitarbeiter untereinander zu erreichen, die zur Verhinderung interner Sabotage oder deren Entdeckung beitragen kann. Solche Strategien greifen nur langsam, bilden aber langfristig den wirksamsten Schutz.

## 4.3.11 Schulung der Mitarbeiter in IT-Sicherheit

Über das allgemeine Sensibilisierungsprogramm hinaus sind Schulungen zu Teilbereichen der IT-Sicherheit erforderlich, wenn sich durch Sicherheitsmaßnahmen einschneidende Veränderungen zum Beispiel im Arbeitsablauf ergeben. Das Schulungsprogramm ist für das jeweilige Unternehmen spezifisch zu entwickeln. Folgende exemplarische Themen können Inhalt dieses Programms sein:

- Sicherheitspolitik und -infrastruktur
- Organisation des IT-Sicherheitsmanagements
- regelmäßige Überprüfung von Sicherheitsmaßnahmen
- bauliche Sicherheit
- Schutz von Gebäuden, Technikräumen und Büroräumen
- Verantwortlichkeiten der Mitarbeiter
- Hardware- und Software-Sicherheit,
- Identifikation und Authentisierung,
- Berechtigungssysteme, Virenschutz.

## 4.3.12 Schulung der Mitarbeiter für Anwendungen

Durch unsachgemäßen Umgang mit IT-Anwendungen hervorgerufene Schäden kann man vermeiden, wenn die Benutzer vor Inbetriebnahme eingehend in die IT-Anwendungen eingewiesen werden.

Aus diesem Grund ist es unabdingbar, dass die Benutzer vor der Übernahme IT-gestützter Aufgaben ausreichend geschult werden. Dies betrifft sowohl die Nutzung von Standardprogrammpaketen als auch von speziell entwickelten IT-Anwendungen. Darüber hinaus muss man auch bei umfangreichen Änderungen in einer IT-Anwendung Schulungsmaßnahmen durchführen.

## 4.3.13 Internet-Nutzung

Um die Gefährdungen, die durch Angriffe aus dem Internet auf lokale Daten oder Rechner im LAN (Local Area Network, lokales Netzwerk) entstehen, zu verringern, ist es erforderlich, Rechner einzusetzen, die nur mit dem Internet vernetzt sind und keine weitere Netzverbindung zu dem LAN haben. Ein unternehmensweites Konzept für die Internet-Nutzung ist festzulegen. Bestandteil dieser Regelung sind unter anderem die Hard- und Software-technische Ausstattung des Arbeitsplatzes, eine Benutzerrichtlinie und das Virenschutzkonzept.

## 4.3.14 Festlegung der Sicherheitspolitik für E-Mail

Vor der Freigabe von E-Mail-Systemen muss festgelegt werden, für welchen Einsatz E-Mail vorgesehen ist. Das Unternehmen muss eine Sicherheitspolitik für den E-Mail-Dienst festlegen, in der folgende Punkte beschrieben sind:

- Wer erhält einen E-Mail-Anschluss?
- Welche Regelungen sind von den Mail-Administratoren und den E-Mail-Benutzern zu beachten?
- Bis zu welchem Vertraulichkeits- beziehungsweise Integritätsanspruch dürfen Informationen per E-Mail versandt werden?
- Ist eine private Nutzung von E-Mail erlaubt, und unter welchen Rahmenbedingungen?
- Wie werden die Benutzer geschult?
- Wie wird jederzeit technische Hilfestellung für die Benutzer gewährleistet?

E-Mails, die intern versandt werden sollen, dürfen das lokale Netz nicht verlassen. Eine Übertragung von E-Mails über das Internet, deren Inhalt einen vertraulichen Charakter hat, sollte auf keinen Fall ohne vorherige Verschlüsselung und eine digitale Signatur erfolgen.

## 4.3.15 Fazit

In einem hochkomplexen System wirken viele Bedrohungen auf die unterschiedlichsten Komponenten ein. Gegen diese Bedrohungen müssen Schutz- und Gegenmaßnahmen aktiviert und gepflegt werden. Um einen hohen Grad an Sicherheit zu erhalten, ist eine weitere Sensibilisierung, nicht nur der Mitarbeiter, sondern auch in den Management-Ebenen der Unternehmen zu etablieren.

Es muss die Aufgabe der Unternehmensführung sein, einen kontinuierlichen Sicherheitsprozess im gesamten Geschäftsbereich zu installieren und ständig weiterzuentwickeln. Dazu muss auch die Einsicht vorhanden sein, dass dieser Prozess mit Hilfe von externen Dienstleistern und der verstärkten Einbindung eigener Kräfte vorangetrieben werden kann.

Darüber hinaus sollte man berücksichtigen, dass wegen unzureichender Maßnahmen im Bereich Organisation und Personal Vorkehrungen im technischen Bereich weit gehend sinnlos werden können.

Detlef Schumann

Der Autor, Dipl.-Wirtsch.-Ing. Detlef Schumann, arbeitete von 1992 bis 2000 als Administrator, DV-Leiter und DV-Koordinator für Unix- und Windows-NT-Umgebungen bei verschiedenen Unternehmen. Seit 2001 ist er als Consultant für die C_sar-Consulting, solutions and results AG tätig. Beim vorliegenden Kapitel handelt es sich um einen Auszug aus dem „Handbuch IT-Sicherheit" (Addison-Wesley 2003), das konzeptionelle und organisatorische Konzepte der IT-Sicherheit behandelt.

**„Handbuch IT-Sicherheit"; Gora, Dr. Walter / Krampert, Thomas (Hrsg.)**; **ISBN 3-8273-2063-1**; 

| tecCHANNEL-Links zum Thema | Webcode | Compact |
|---|---|---|
| Security im Überblick | a1068 | – |
| Webdienste und Sicherheit | a1088 | – |
| VPN – Daten sicher übers Internet | a306 | – |
| Sicherheit im WLAN | a928 | – |
| Firewall-Grundlagen | a682 | – |
| Lauschangriff im Firmennetz | a288 | – |
| Die Netzwächter | a600 | – |

# Glossar

## ACL

Access Control List. Unter Windows NT/2000/XP eine Liste mit Zugriffsrechten für Benutzer und Gruppen auf Dateien, Verzeichnisse oder andere Objekte des Betriebssystems.

## ActiveX

Software-Modul, das auf der „Component Objekt Model“-Architektur von Microsoft basiert. Über ActiveX-Controls lassen sich bestehende Software-Komponenten von einem Server abrufen und im Webbrowser wie ein normales Programm anwenden.

## AH

IP Authentication Header (RFC 2402). Ermöglicht, die Integrität und Authentizität von Datenpaketen bei der IPsec-Übertragung zu prüfen.

## ANSI

American National Standards Institute. Institut in den USA zur Normierung von diversen technischen Spezifikationen. Vergleichbar mit dem DIN in Deutschland.

## API

Application Programming Interface. Spezifizierte Schnittstelle zu Funktionen in einer Anwendung oder einem Betriebssystem. Damit lassen sich häufig benutzte Funktionen, wie etwa das Formatieren von Texten oder das Darstellen von Fenstern, in einer zentralen DLL unterbringen.

## Backbone

Rückgrat. In der Kommunikationstechnologie wird dieser Begriff für den zentralen Teil des Netzwerks verwendet, über den ein Großteil des Datenverkehrs läuft. Ein Collapsed Backbone komprimiert die Backbone-Funktion in der Backplane eines Core Switch.

## Backdoor

Hintertür in Form eines offenen Ports, den sich Trojaner-Programme (siehe: Trojaner) für das Eindringen in einen Rechner offenhalten.

## BIOS

Basic Input Output System: Programmroutine, die im ROM eines Rechners untergebracht ist und beim Booten die angeschlossene Hardware überprüft.

## Bootsektor

Der erste logische Sektor einer Festplatte. Er enthält neben Informationen über das verwendete Medium wie Größe und Cluster-Zahl ein Startprogramm, das für das Booten des jeweiligen Betriebssystems zuständig ist.

## Brute-Force

Brute-Force-Angriff: Das Anwenden brutaler Gewalt – also der Versuch, ein Kryptosystem durch das Ausprobieren aller möglichen Schlüssel-Kombinationen zu brechen. Der Aufwand, durch einen Brute-Force-Angriff ein System zu knacken, stellt eine obere Grenze für die Stärke eines Algorithmus dar. Die Stärke eines Kryptosystems gilt als optimal, wenn es keinen möglichen Angriff auf das System gibt, der weniger aufwendig als ein Brute-Force-Angriff wäre.

## CA

Certification Authority. Zertifizierungsstelle, Trust Center: CAs liefern Schlüssel und digitale Zertifikate für den rechtsverbindlichen und vertraulichen Datenverkehr.

## CHAP

Challenge Handshake Authentication. Verfahren zur Authentifizierung bei Einwählverbindungen. Der Server sendet zur Verbindungsaufnahme zunächst eine spezielle Code-Sequenz (Challenge), auf die der Client richtig antworten muss (Handshake).

## COM

Component Object Model: Erlaubt es Programmierern, Objekte zu entwickeln, die von jeder COM-kompatiblen Anwendung genutzt werden können. ActiveX-Controls basieren beispielsweise auf COM. Weitere Informationen finden Sie auf Microsofts COM-Seiten unter http://www.microsoft.com/com/default.asp

## CRC

Cyclical Redundancy Checking. Eine sehr sichere Methode, Übertragungsfehler bei einem Datentransfer festzustellen.

## DCF

Distributed Coordination Function. Medienzugriffsregelung in drahtlosen Netzen nach IEEE802.11-Standard.

## DDE

Dynamic Data Exchange. Ein System zum dynamischen Datenaustausch unter Windows und anderen Betriebssystemen. DDE ermöglicht es zwei aktiven Anwendungen, auf gemeinsame Daten zuzugreifen. DDE wurde mittlerweile in vielen Bereichen von dem flexibleren OLE (Object Linking and Embedding) abgelöst.

## DES

Data Encryption Standard. Ein Verschlüsselungsverfahren mit Secret-Key-Technik. Das Standardverfahren verwendet eine Schlüssellänge von nur 56 Bit. Daher verwendet der TripleDES drei Schlüssel mit je 56 Bit, um die Sicherheit zu erhöhen.

## DHCP

Dynamic Host Configuration Protocol. Protokoll zur automatischen Vergabe von IP-Adressen. Bei DHCP bezieht ein Arbeitsrechner seine Konfiguration des IP-Netzwerks von einem Server.

## DIFS

Distributed Interframe Space. Wartezeit für sendewillige 801.11-Stationen vor Aufnahme der Datenübertragung.

## DIMMs

Dual Inline Memory Module: Speichermodul mit Kontaktflächen auf beiden Seiten der Platine, die elektrisch getrennt sind. Die 168-poligen DIMMs haben eine Datenbreite von 64 Bit.

## DirectX

Eine Microsoft-Programmbibliothek mit Schnittstelleninformationen unter anderem zur optischen und akustischen Darstellung von 3D-Informationen von Spielen.

## DMZ

Demilitarized Zone, entmilitarisierte Zone: Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. Das DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.

## DNS

Domain Name System (oder Service). Ein Internet-Dienst, der Domain-Namen wie www.tecChannel.de in die zugehörigen IP-Adressen umsetzt. Die Umsetzung erfolgt in einer hierarchischen Struktur von DNS-Servern. Kann ein DNS-Server die IP-Adresse eines Namens nicht selbst auflösen, so fragt er bei einem übergeordneten Server nach. An der Spitze stehen die so genannten Root-Server.

## Domäne

Als Domäne (Domain) bezeichnet der Hersteller Microsoft eine Gruppe von Netzwerkressourcen (Rechner, Drucker, Verzeichnisse, Anwendungen usw.), die über einen gemeinsamen Authentifizierungsmechanismus für Benutzer freigegeben werden. Als Domain Controller bezeichnete Server stellen die dazu notwendigen Sicherheitsmechanismen zur Verfügung. Rechner, die an der Domänensicherheit teilnehmen wollen, müssen dazu der Domäne beitreten. Nicht zur Domain gehörende Rechner können zwar einzelne Freigaben nutzen, nicht aber alle Mechanismen der Domäne.

## DoS

Denial of Service. Hacker-Angriff auf einen Rechner, der nur ein Ziel hat: den angegriffenen Computer lahmzulegen, so dass er auf Anfragen nicht mehr reagieren kann. Erfolgt ein DoS-Angriff koordiniert von mehreren Rechnern aus gleichzeitig, spricht man von DDoS (Disributed Denial of Service.)

## DSL

Digital Subscriber Line. Die Standleitung ins Internet für kleine Firmen und Privatpersonen. DSL arbeitet mit denselben Kupferkabeln wie analoge Telefone und ISDN-Anschlüsse. Die Übertragungsgeräte (Splitter und DSL-Modem) sind jedoch aufwendiger. Man unterscheidet zwischen ADSL (Asymmetrisches DSL, verschiedene Up- und Downstream-Datenraten) und SDSL (Symmetric DSL, identische Transfergeschwindigkeit von und zum Internet.)

## DSSS

Direct Sequence Spread Spectrum. Bandspreizverfahren, das auf der Aufteilung der Sende-Energie über das verfügbare Frequenzband beruht. DSSS ist besonders resistent gegen Abhören und schmalbandige Störeinflüsse.

## Dual-Homed

Bei dieser Variante befindet sich der Firewall-Rechner, bestehend entweder aus einem Paketfilter-Router oder einem Application Level Gateway, zwischen dem Firmennetz und dem Internet. Dieser Aufbau erleichtert zwar die Implementierung, der potenzielle Angreifer muss aber auch nur eine einzige Hürde überwinden. Ihren Namen hat die Variante von der Notwendigkeit, der Firewall zwei Netzschnittstellen zu geben, so dass sie in zwei Netzen zu Hause ist (dual-homed).

## ECC

Error Correcting Code: ein Verfahren zum Erkennen und Korrigieren von Bitfehlern.

## ESP

IP Encapsulated Security Payload (RFC 2406). Sorgt mittels eines Headers und Trailers für die verschüsselte Übermittlung der Nutzdaten über IPsec-Verbindungen.

## Ethernet

Die am weitesten verbreitete Methode zur Vernetzung in einem LAN. Verbindungen lassen sich über Twisted-Pair-Kabel, Glasfaser oder Koaxial-Kabel herstellen. Nach der Geschwindigkeit unterscheidet man Ethernet (10 Mbit/s), Fast Ethernet (100 Mbit/s), Gigabit-Ethernet (GE, 1 GBit/s) und 10-Gigabit-Ethernet (10GE, Gbit/s).

## ETSI

European Telecommunications Standardisation Institute. Europäisches Standardisierungsinstitut für Telekommunikation.

## Firewall

Software zur Sicherung des LAN vor Angriffen aus dem Internet. Eine Firewall kann auf verschiedenen Ebenen arbeiten: Als Paketfilter erlaubt sie lediglich Zugriffe auf bestimmte lokale IP-Adressen und Ports. Als Proxy-Server agiert sie als Kommunikations-Schnittstelle. Der Client im LAN leitet seine Anfragen nicht direkt an den Zielserver, sondern über den Proxy. Mit Stateful Inspection überwacht sie nicht nur den reinen Datenverkehr, sondern auch die Anwendungsebene des OSI-Schichtenmodells.

## Flash

Nichtflüchtiges Halbleitermedium, das wie ein EEPROM (Electrical Erasable Read Only Memory) elektrisch beschrieben und gelöscht werden kann. Bei Flash-Speichern ist nicht jedes einzelne Bit adressierbar, die Zugriffe erfolgen auf Sektorebene ähnlich wie bei Festplatten.

## FTP

File Transfer Protocol. Spezielles IP-Protokoll auf UDP-Basis zur Übertragung von Dateien.

## GUI

Graphical User Interface. Oberbegriff für grafische Benutzeroberflächen wie Windows oder X-Windows.

## Hashing

Hash von Hashing-Algorithmus. Ausgehend von einer Datenmenge wird ein eindeutiger nummerischer Wert erzeugt. Jede Veränderung der Datenbasis führt zu einer Veränderung des Hash-Werts.

## HTML

HyperText Markup Language. Diese Seitenbeschreibungssprache ist Grundlage jeder Webseite. Der HTML-Standard wird vom W3C verwaltet. Wird künftig durch das XML-basierte XHTML ersetzt.

## HTTP

HyperText Transport Protocol. Dient zur Übertragung von Webseiten zwischen Webserver und Browser.

## HTTPS

HyperText Transport Protocol Secure. Dient zur sicheren Übertragung von Webseiten zwischen Webserver und Browser. Die Kommunikation erfolgt SSL-verschlüsselt über Port 443 statt Port 80 wie für herkömmliches HTTP.

## IANA

Internet Assigned Numbers Authority. Zeichnet für die Administration des Domain Name System (DNS) verantwortlich. Regelt über regionale Registrare wie APNIC, ARIN oder RIPE die Vergabe von IP-Adressen und Top Level Domains (TLDs).

## ICMP

Internet Control Message Protocol. Bestandteil der TCP/IP-Protokollsuite. ICMP dient dabei zum Austausch von Fehler- und Status-Meldungen.

## IEEE

Institute of Electrical and Electronic Engineers. Eine in den USA ansässige Ingenieurvereinigung zur Erstellung von Standards und Normen. Entspricht in etwa dem deutschen VDE.

## IGMP

Internet Group Management Protocol (RFC 2236). IGMP zählt zum OSI-Netzwerk-Layer und ermöglicht es Routern, Informationen über die Multicast-Gruppenzugehörigkeit von Rechnern zu erhalten.

## IMAP4

Internet Mail Access Protocol, Version 4. Standard-Protokoll zur Zustellung von E-Mails. E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server. Im Gegensatz zu POP3 bleiben bei IMAP4 die Nachrichten standardmäßig auf dem Server.

## IP

Internet Protokoll. Bestandteil der TCP/IP-Suite. IP sendet die Daten in Paketen (auch Datagramme genannt) an die Empfängeradresse. Es kümmert sich jedoch nicht darum, ob die Daten wirklich ankommen. Dafür ist der TCP-Bestandteil zuständig. Derzeit ist IP Version 4 im Einsatz. IP Version 6 (auch IP Next Generation) zur Erweiterung des verfügbaren Adressraums ist bereits verabschiedet, wird bislang jedoch noch wenig eingesetzt.

## IPsec

Security Architecture for IP (RFC 2401). Architektur für die sichere Datenübertragung via IPv4 und IPv6. Umfasst Protokolle, Algorithmen und Verfahren für die Schlüsselverwaltung (RFC 2402-2412).

## IRC

Internet Relay Chat. Chat-System zur Echtzeitkommunikation.

## IrDA

The Infrared Data Association. Standard zur Datenübertragung per Infrarot. In der Version 1.0 mit Geschwindigkeiten bis zu 115 Kbit/s, seit der Version 1.1 (Fast IrDA) mit bis zu 4 Mbit/s.

## ISDN

Integrated Services Digital Network. Digitales Übermittlungsverfahren, das verschiedene Dienste wie Telefonie oder Datenaustausch im Verbund ermöglicht.

## ISO

Internationale Normungsorganisation für vorwiegend nicht elektrische und nicht elektronische Normen in Genf. Die Kurzbezeichnung ist nicht die Abkürzung für die Organisationsbezeichnung, sondern wird aus Griechisch „iso“ (gleich = Norm) abgeleitet.

## ITU

International Telecommunication Union. Internationale Organisation zur Koordinierung von TK-Netzen und Diensten. 1865 gegründet, seit 1947 als Teil der UN in Genf ansässig. ITU besteht seit 1994 aus den drei Sektoren Radiocommunication (ITU-R), Telecommunications Standardization (ITU-T) und Telecommunications Development (ITU-D). Die ITU gibt so genannte Empfehlungen (Recommendations) in verschiedenen, von A bis Z durchbuchstabierten Serien heraus. Die bekanntesten davon sind die G-Serie (Übertragungstechnik), die Q-Serie (Telefonie), die V-Serie (Datenübertragung) sowie die X-Serie (Datennetze).

## Java

Von Sun entwickelte, spezifizierte und überwachte plattformunabhängige Programmiersprache. In Java entwickelte Programme werden für eine virtuelle Prozessorarchitektur kompiliert. Der resultierende Byte-Code lässt sich unter jedem Betriebssystem verwenden, für das eine entsprechende Implementation des virtuellen Java-Rechners („Java Virtual Machine“) verfügbar ist.

## Javascript

Script-Sprache zur Programmierung einfacher Funktionen. Das Script ist gewöhnlich in die HTML-Seite integriert und wird innerhalb der Browser-Umgebung ausgeführt. Trotz seines Namens ist Javascript weder verwandt noch kompatibel zu Java. Ein Subset der ursprünglich von Netscape entwickelten Script-Sprache ist mittlerweile als ECMAscript standardisiert.

## JDBC

Java Database Connectivity: Schnittstelle für den Zugriff aus Java-Programmen auf beliebige relationale Datenbank-Systeme. Dabei abstrahiert JDBC den Zugriff von der konkreten RDBMS-Implementation. Ein vom Datenbankhersteller oder einem Dritten bereitgestellter JDBC-Treiber übernimmt den eigentlichen Zugriff.

## Kerberos

Sicherheitsstandard des MIT zur zentralen Authentifizierung von Benutzern (single-logon). Kerberos ist nicht für die Freigabe von Ressourcen zuständig, sondern es weist einem Benutzer lediglich eine ID zu, die während der Sitzung erhalten bleibt. Über diese ID können dann die einzelnen Ressourcen entscheiden, welche Rechte der Benutzer erhält.

## LAN

Lokal Area Network. Netzwerk aus Computern und Geräten an einem Standort. Vergleiche MAN, WAN.

## LDAP

Lightweight Directory Access Protocol. Standardisiertes Netzwerkprotokoll zum Zugriff auf Verzeichnisdienste, über die sich Ressourcen wie E-Mail-Adressen finden lassen.

## Malware

Allgemeiner Sammelbegriff für alle Programme, die Daten zerstören, manipulieren oder ausspähen.

## MAC

Message Authentication Code. Durch ein Hash-Verfahren generierter Wert fester Länge, der unter anderem zur Überprüfung der Echtheit einer Nachricht dienen kann.

## MAN

Metropolitan Area Network. Regional- oder Stadtnetz. Üblicherweise bezeichnet man WANs mit einer Ausdehnung unter 100 km Radius als MANs.

## MAPI

Messaging Application Programming Interface: Von Microsoft definierte Schnittstelle, mit der von jeder Windows-Software aus E-Mails verschickt werden können.

## MBR

Der Master Boot Record ist der erste physikalische Sektor einer Festplatte. In diesen 512 Byte sind der Bootloader und die Partitionstabelle untergebracht.

## MD5
Message-Digest-Algorithmus: Version 5 ist ein Verschlüsselungsalgorithmus, der zur Erzeugung digitaler Signaturen verwendet wird.

## MIME
Multipurpose Internet Mail Extensions: Erweiterung der textbasierten E-Mail um Verfahren für den Versand von Binärdateien, Grafik-, Video- und Audio-Daten.

## MTBF
Mean Time Between Failures. Die mittlere Zeitspanne zwischen Fehlern. MTBF dient zur Kennzeichnung der Zuverlässigkeit eines Geräts und ist als Durchschnittswert anzusehen.

## MTU
Maximum Transfer Unit. Die maximal zulässige Größe eines Netzwerkpaketes in Byte. Überschreitet ein Datenpaket die MTU, wird es beim Transport im Netz fragmentiert und unter Umständen nicht korrekt transportiert.

## NAT
Network Address Translation. NAT ist ein Verfahren zur Abschottung des LAN gegenüber dem Internet. Dabei wird zum Internet hin immer nur eine Adresse gemeldet, unabhängig von der tatsächlichen IP-Adresse des Absenders im LAN. Der NAT-Router übernimmt dabei die Verteilung der eintreffenden IP-Pakete zu den richtigen Empfängern.

## NAV
Net Allocation Vector. Zeitgeber für den RTS-CTS-Mechanismus in 802.11-Netzen.

## NDS
Novell Directory Services: Verzeichnisdienst von Novell, welcher mit Netware 4.0 eingeführt wurde und eine netzwerkweite hierarchische Ablage von Objektinformationen in einer Datenbank ermöglicht. Die Definition von Ressourcen, etwa Druckern, Benutzern oder Servern, erlaubt es Administratoren, Anwender durch eine einzige Authentifizierung zu verwalten.

## NetBIOS
Network Basic Input Output System: Protokoll in DOS- und Windows-Netzwerken. Das ursprünglich von IBM entwickelte NetBIOS stellt eine Programmierschnittstelle für Applikationen zur Verfügung, die auf Schicht 5 des OSI-Modells arbeiten. NetBIOS setzt auf dem nicht Routing-fähigen Transportprotokoll NetBEUI auf. Um ein Routing zu erzielen, wird NetBIOS in manchen Implementationen über die Protokolle TCP/IP (Microsoft) und IPX/SPX (Novell) gekapselt.

## NNTP
Kurz für Network News Transport Protocol. In RFC977 beschriebenes Protokoll zur Übertragung von USENET-Nachrichten. Die Nachrichten des USENET sind in schwarzen Brettern (so genannten newsgroups) organisiert.

## NTFS

NT File System. In Windows NT implementiertes Dateisystem, das unter NT 3 und 4 auch Partitionen und Dateien über 4 Gigabyte ermöglicht. Windows 2000 besitzt dafür auch das FAT32-Filesystem. NTFS ermöglicht erweiterte Zugriffsrechte und bietet eine erhöhte Sicherheit.

## OLE

Object Linking and Embedding. Über OLE lassen sich beispielsweise Excel-Dokumente direkt in Word einbinden und dennoch mit den Werkzeugen von Excel weiter bearbeiten.

## OSI-Modell

Open Systems Interconnect. Ein ISO-Standard für weltweite Kommunikation, der ein Rahmenmodell für die Implementierung von Protokollen in sieben Schichten definiert.

## Partition

Logische Unterteilung einer Festplatte in einen Satz zusammenhängender Sektoren.

## Payload

Wörtlich: Nutzlast. Programmierte Schadensfunktionen von Malware, die beim Eintreten eines bestimmten Ereignisses (etwa Datum, Uhrzeit oder Anwenderaktion) aktiviert werden. Daher wäre eigentlich der Ausdruck „Schadlast“ passender.

## PKI

Public Key Infrastructure. Infrastruktur für den Einsatz von Verschlüsselungs- und Signaturdiensten. Regelt die Erstellung, Zuordung, Verteilung, Verwaltung, Prüfung und Rücknahme von Schlüsseln und Zertifikaten.

## Plug-ins

Plug-ins sind Code-Bestandteile für Zusatzfunktionen, die man in ein bereits vorhandenes Hauptprogramm hineinlädt. Sie stehen dann in einem neuen Untermenü zur Verfügung. Beliebte Einsatzgebiete sind Webbrowser-Erweiterungen oder Spezialeffekte für Bildbearbeitungsprogramme.

## POP3

Post Office Protocol, Version 3. Standard-Protokoll zur Zustellung von E-Mails. E-Mail-Clients wie Outlook, Netscape Messenger und Eudora verwenden das Protokoll zur Kommunikation mit einem E-Mail-Server.

## Port

Ein Port dient als Kommunikationskanal für den Zugriff auf einen Internet-Rechner über das TCP/IP-Protokoll, ähnlich den Nebenstellen eines Telefonanschlusses. Jedes TCP/IP-Programm verwendet einen Port für die Kommunikation mit anderen Rechnern. Je nach verwendetem Protokoll unterscheidet man zwischen TCP- und UDP-Ports.

## PPP

Point-to-Point Protocol. Gebräulichstes Einwahlverfahren für den Zugriff auf entfernte Netze, wie das Internet.

## PPPoE

Point-to-Point-Protocol over Ethernet. Spezielles Protokoll, das Punkt-zu-Punkt-Verbindungen über das Ethernet ermöglicht. Kommt meist in Verbindung mit DSL zum Einsatz.

## Proxy

Meist als Kurzform für Proxy-Cache verwendet. Dabei handelt es sich um eine Komponente des Proxy-Servers einer Firewall. Der Cache speichert beispielsweise Internet-Seiten lokal zwischen, so dass sie beim nächsten Abruf nicht vom Internet-Server geholt werden müssen, sondern schneller und kostengünstiger aus dem lokalen Cache.

## RAID

Redundant Array of Independent Discs. Ein Konzept, eine Anzahl von Festplatten zur Erhöhung der Übertragungsleistung und technischen Sicherheit als eine Einheit zu betreiben. Aus Sicht von SCSI kann ein RAID aus mehreren Laufwerken (Targets) an einem oder mehreren Steuereinheiten (Initiators) oder aus mehreren LUNs in einem Target aufgebaut sein. Die Steuerung eines RAID übernimmt ein entsprechender Controller. Nach dem verwendeten Verfahren zur Zusammenfassung der Einzellaufwerke unterscheidet man zwischen den so genannten RAID-Levels 0 bis 7.

## RC4

Verschlüsselungsverfahren von RSA Data Security. Es arbeitet mit einem geheimen Schlüssel und einer variablen Schlüssellänge. Das bereits 1987 entwickelte Stromverschlüsselungsverfahren kommt in zahlreichen kommerziellen Produkten zum Einsatz, wie etwa Lotus Notes, Oracle Secure SQL oder Netscape Navigator.

## RFC

Request for Comments: Sammlung von Empfehlungen, Artikeln und Standards der Internet Engineering Task Force (IETF). RFCs halten netzrelevante Konventionen und allgemeine Informationen zum Internet fest.

## Router

Router vermitteln die Daten zwischen zwei oder mehreren (Sub-)Netzen, die beispielsweise durch Weitverkehrsleitungen wie ISDN verbunden sind. Auch im LAN ist ein Einsatz von Routern möglich, um Teilnetze logisch zu trennen sowie die Datensicherheit zu erhöhen.

## RPC

Remote Procedure Call. Programmierschnittstelle, mit der Funktionen auf entfernten Rechnern ausgeführt werden können. RPCs wurde von Sun für die „Open Network Computing“-Architektur entwickelt. Eine weitere RPC-Architektur ist Microsofts DCOM.

## RSA

RSA (Rivest, Shamir, Adelman): Verschlüsselungsverfahren, bei dem jeder Partner einen allgemein bekannten (public) und einen geheimen (private) Schlüssel besitzt. Unterschiedliche Implementierungen des Verfahrens nutzen verschiedene Schlüssellängen. Als unsicher gelten derzeit Schlüssellängen von unter 1024 Bit.

## RTF

Rich Text Format. Plattformunabhängiges Dateiformat zur Speicherung von Dokumenten.

## SA

Security Association, diese ist Teil des Internet Security Association and Key Management Protocol (ISAKMP, RFC 2408/2409). Bezeichnung für eine zwischen zwei Endstellen verhandelte Kommunikationsbeziehung im Rahmen von IPsec.

## SIFS

Short Interframe Space. Wartezeit für sendewillige 802.11-Stationen vor Beginn einer Empfangsquittierung.

## SMB

Server Message Block. Netzwerkprotokoll auf Schicht 6/7 des OSI-Modells. Bietet Mechanismen zur Freigabe von Dateien, Druckern und Kommunikationsschnittstellen. Definiert abstrakte Kommunikation über named pipes und mail slots. Benötigt zur Datenübertragung ein Transportprotokoll wie TCP/IP oder NetBEUI.

## SMTP

Simple Mail Transfer Protocol. Standardprotokoll zum E-Mail-Versand. E-Mail-Server verwenden das Protokoll zur Kommunikation untereinander.

## Social Engineering

Gezielte Beeinflussung anderer, um unter Ausnutzung menschlicher Eigenheiten und Schwächen unberechtigt an Informationen zu gelangen oder ein bestimmtes Verhalten des Anwenders zu forcieren. Dies kann auf verschiedenste Art und Weise geschehen, etwa indem sich jemand als Autoritätsperson (Systemadministrator, Support-Mitarbeiter) ausgibt und den User zur Herausgabe seines Passworts auffordert. Oder ganz einfach per E-Mail, deren Betreffzeile (I love you) den Nutzer zum arglosen Öffnen des (virenverseuchten) Attachments bewegt.

## SSH

Secure Shell. Ein von der Firma SSH Communications Security entwickeltes Programm, das eine sichere Kommunikation und Authentifizierung ermöglicht. Dazu verschlüsselt SSH den kompletten Login-Prozess einschließlich der Passwortübermittlung. SSH steht unter anderem für Windows und Unix zur Verfügung.

## SSID

Shared System ID. Manchmal auch als Shared Key bezeichnet. Gemeinsamer Schlüssel für den Zugriff auf ein Wireless LAN nach IEEE-802.11-Standard.

## SSL
Secure Sockets Layer. Von Netscape eingeführtes Protokoll zur Übermittlung von privaten Informationen. Verwendet ein Public-Key-Verfahren für die Verschlüsselung.

## TCP
Transmission Control Protocol. Verbindungsorientiertes Transportprotokoll aus der TCP/IP-Suite. Umfasst Verbindungsauf- und -abbau, Reihenfolgegarantie, Verlustsicherung, Flusskontrolle und anderes mehr.

## TCP/IP
Transport Control Protocol/Internet Protocol. Die am meisten verbreitete Netzwerk-Protokollsuite zur Übermittlung von Daten. Das Internet Protocol (IP) dient zum verbindungslosen Datentransport. Das Transmission Control Protocol (TCP) stellt sicher, dass die Daten auch fehlerfrei ankommen.

## Telnet
Telnet ermöglicht den Zugriff auf die Kommandoebene eines entfernten Rechners.

## TLS
Transport Layer Security: Weiterentwicklung von Secure Sockets Layer (SSL). TLS ist in RFC 2246 definiert und sorgt für Sicherheit und Datenintegrität zwischen zwei Anwendungen.

## Trigger
Ein Trigger ist ein Auslösemechanismus, der beim Eintreten einer vorher festgelegten Bedingungen eine konfigurierbare Aktion auslöst. Schadsoftware verwendet oft Trigger, um die Auslösung der Schadfunktion bis zu einem bestimmten Datum zu verzögern.

## Trojaner
Ein Trojanisches Pferd, kurz Trojaner, erscheint als vermeintlich nützliches Programm, etwa als Utility. So getarnt, wird es von arglosen Anwendern verbreitet und benötigt daher keinen eigenen Replikationsmechanismus. Trojaner werden bevorzugt eingesetzt, um Daten auf fremden Rechnern auszuspähen. Aber auch für jede andere Form der Datenmanipulation lassen sie sich einsetzen.

## Trust Center
Alternative Bezeichnung für Certification Authority (siehe: CA).

## TTL
Time to live: Angabe im Internet Protocol (IP), die bestimmt, nach wie vielen Hops (Passieren einzelner Router) ein Paket als unzustellbar verworfen wird.

## Tunneling
Kapseln der Datenkommunikation eines Protokolls innerhalb eines anderen Protokolls, so dass dieses quasi als Transportschicht für das getunnelte fungiert.

## UDP

User Datagram Protocol, Teil der TCP/IP-Protokollsuite. Das verbindungslose UDP erlaubt das Versenden von Datenpaketen („Datagrammen“) zwischen zwei Systemen. Das Protokoll garantiert weder die Zustellungen, noch die korrekte Reihenfolge der zugestellten Datenpakete. Dient typischerweise zum Transport geringer Datenmengen, bei denen der Verwaltungs-Overhead einer verbindungsorientierten Übertragung den Aufwand einer gegebenenfalls notwendigen Retransmission übersteigen würde.

## UNC

Universal Naming Convention. Konvention zur Benennung von Ressourcen (Drucker, Shares etc.) auf Netzwerkservern. Unter DOS/Windows werden Namen mit \\servername\ressourcenname angegeben, unter Unix mit //servername/ressourcenname.

## VBS

Visual Basic Script: Script-Sprache von Microsoft, die mit Visual Basic verwandt ist. Visual Basic Script findet nicht nur Verwendung in Webseiten, sondern kann auch lokal vom Windows Scripting Host interpretiert werden.

## VBScript

Sammelbegriff von Microsoft für die Script-Sprachen JScript (Microsofts Variante von JavaScript) und das Visual-Basic-basierte VBScript.

## Viren

Ein Computervirus ist ein Programm, das zu seiner Weiterverbreitung fremden Code infiziert. Dies können neben Anwender- und Programmdateien auch Systembereiche auf Speichermedien sein. Darüber hinaus besitzt ein Virus meist eine Schadensroutine, die von störenden Bildschirmanimationen bis zum Löschen von Dateien reicht.

## Visual Basic Script

Sammelbegriff von Microsoft für die Script-Sprachen JScript (Microsofts Variante von JavaScript) und das auf Visual-Basic basierende VBScript.

## VPN

Virtual Private Network. Beim VPN lassen sich über ein öffentliches Datennetz, wie etwa das Internet, sichere private Verbindungen, beispielsweise in das Firmennetz, aufbauen. Mit VPNs lassen sich zwei Netze koppeln oder mobile Anwender („Roadwarriors“) über das Internet an die Unternehmens-DV ankoppeln. Als Protokoll für VPNs kommt inzwischen weit gehend das standardisierte IPsec zum Einsatz.

## WAN

Wide Area Network. Computernetzwerk, das über Telefon-, Funk- oder andere Weitverkehrsverbindungen kommuniziert. Das größte WAN ist das Internet. Vgl. LAN, MAN.

## WebDAV

Web Distributing, Authoring and Versioning: Technik zur einfachen Veröffentlichung von Websites. WebDAV besteht aus HTTP-Erweiterungen, die einen standardisierten Datenaustausch zwischen Web-Authoring-Tools und Servern gestatten.

## WEP

WEP, Wireless Equivalent Privacy. Bezeichnung für Verschlüsselungsverfahren auf RC4-Basis, die von auf dem Standard 802.11 basierenden Funknetzen genutzt werden. Gilt mittlerweile auf Grund von Implementierungsschwächen als unsicher.

## WINS

Windows Internet Naming Service: Dienst zur Namensauflösung, der bei Microsofts Server-Betriebssystemen die Umsetzung von NetBIOS-Namen auf IP-Adressen vornimmt.

## WLAN

Wireless LAN. Allgemein: Drahtloses lokales Netzwerk auf Funk- oder Infrarot-Basis. Hat sich inzwischen als Umschreibung für Funknetze nach dem IEEE-Standard 802.11 eingebürgert.

## Würmer

Ein Computerprogramm, dessen einzige Aufgabe es ist, sich selber zu reproduzieren und zu verbreiten. Im Gegensatz zu einem Virus infiziert ein Wurm keine anderen Programme und ist auf die selbstständige Verbreitung in Netzwerken ausgerichtet. Den ersten Internet-Wurm brachte Robert Morris 1988 in Umlauf. Sein Programm legte über 6000 Computer lahm, weil sie nur noch mit der Verbreitung des Wurms beschäftigt waren.

## X.509

ISO/IEC/ITU-Standard für die Public Key Infrastructure (PKI). Siehe auch RFC 2459. Ein X.509-Zertifikat ordnet einen Public Key eindeutig seinem Inhaber zu. Das Zertifikat beinhaltet Daten über den verwendeten Signaturalgorithmus, den Aussteller, den Inhaber und die Gültigkeitsdauer. Als wichtigste Information enthält es den Public Key des Inhabers. Für die Glaubwürdigkeit des Zertifikats steht dessen Aussteller gerade, die Certification Authority (CA).

## Zertifikate

Quasi-Standard für die Definition digitaler Zertifikate. X.509 ist bislang nur eine Empfehlung der ITU, also noch kein international anerkannter Internet-Standard. Liegt beispielsweise den SSL-Implementierungen von Microsofts und Netscapes Webserver zu Grunde.

# Index

## L



## M



## N



## P



## R



## S



## T



## U



## V



## W



## X